REPUBLIQUE DU CAMEROUN
****
Paix -Travail-Patrie
****
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
****

INSTITUT UNIVERSITAIRE DE LA COTE
****
Institut d'Ingénierie Informatique d'Afrique Centrale
****
DEPARTEMENT DU CYCLE MASTER CS2I
****

DETECTION / PREVENTION AUTOMATIQUE D'INTRUSIONS A PARTIR DE CAPTEURS DISTRIBUES DANS UN RESEAU INFORMATIQUE. Cas d'étude : IP-TELRA

Mémoire de fin d'études

Rédigé et soutenu par **:**

TIOWA NZONTEU

Matricule : **ISTDI15E010728**

En vue de l'obtention du :

Diplôme de Master des Systèmes d'Information et d'Infrastructures, Expert Réseau Infrastructure et Sécurité

Sous la direction de :

Superviseur : **Dr. AZEUFACK Ulrich**

Encadreur Académique : **M. KITIO VOUKENG**

Encadreur Professionnel : **M. TCHOFO Daryl**

Devant un jury composé de :

Président : **Dr. TEGUIA Jean Blaise**

Rapporteur : **M. TEKEU Hypolithe**

Examinateur : **M. HAMENI Christian**

Année Académique : 2021-2022

DEDICACE

A
La Famille TIOWA

REMERCIEMENTS

Nous tenons à adresser toute notre gratitude et nos sincères remerciements aux personnes qui ont contribué à la réussite de notre formation et de ce projet. Nos remerciements vont plus particulièrement à l'endroit de :

- ✓ Monsieur **GUIMEZAP Paul** fondateur d'IUC, pour avoir mis sur pied le pôle de l'excellence académique et nous avoir accueillis au sein de son établissement.
- ✓ Monsieur **NWOKAM Verlaine** à la tête du département CS2I 3IL au seins d'IUC, pour son dévoiement dans sa tâche.
- ✓ Dr. **AZEUFACK Ulrich** mon superviseur pour sa disponibilité, ces précieux conseils et son engagement dans le travail.
- ✓ Monsieur **KITIO VOUKENG** mon encadreur académique, pour tout le travail d'encadrement effectué et la disponibilité qu'il nous porte.
- ✓ Tous nos enseignants pour les connaissances acquises et aussi pour leurs dévouements taches d'enseignement.
- ✓ Monsieur **TCHOFO Daryl** mon encadreur professionnel, pour tout le travail effectué ainsi que la confiance et l'engagement dans le travail.
- ✓ Tous nos collègues de service pour l'aide apporté et l'accueil au sein du groupe IP-TELRA.
- ✓ Nos très chers et tendres parents pour leur soutien moral et matériel.
- ✓ Tous nos camarades pour le soutien, la solidarité et l'aide perçus tout au long de l'année.
- ✓ Tous les jurys de pré soutenance que nous avons eu qui ont permis d'améliorer notre mémoire et combler certaines lacunes.
- ✓ Tous les membres du jurys ici présents pour avoir pris de leurs temps pour évaluer ce travail.

Et tous ceux qui n'ont pas pu être mentionné plus haut.

SOMMAIRE

RESUME

Dans ce travail, en vue d'augmenter le niveau de sécurité de l'entreprise IP-TELRA qui jusqu'ici ne possédait qu'une sécurité informatique et réseau minimale ne garantissant pas au mieux la sécurité des données et des ressources de l'entreprise, nous proposons une architecture distribuée de détection et de prévention d'intrusions basée sur le système de détection d'intrusions réseau Bro (devenu Zeek depuis 2018), pour les réseaux de grande étendue en général et le réseau de l'entreprise IP-TELRA en particulier. Le réseau de l'entreprise IP-TELRA propose plusieurs services parmi lesquelles l'interconnections de certaines structures afin de leurs donner accès à Internet et certaines ressources. IP-TELRA se doit alors de disposer de meilleurs outils en matière de sécurité pour continuer d'assurer une bonne qualité de service. Dans l'architecture distribuée de détection et de prévention d'intrusions que nous proposons pour ce réseau, chaque entité communique au moment opportun avec les autres entités en vue d'un partage d'événements importants. Aussi, nous proposons un réseau de pots de miel (honeynet) pour l'étude des outils et comportements des pirates pour adapter nos règles et mesures de sécurité afin de rentre la sécurité au sein d'IP-TELRA encore plus robuste. Ce réseau de pots de miel est réalisé de façon à reproduire l'environnement de production du réseau dans le but de rassembler des données sur les attaques qui viseraient les serveurs du réseau. A la fin de notre investigation nous avons pu mettre en place un système de détection et prévention d'intrusion en utilisant le système de prévention et de détection d'intrusion bro couplé à un réseau pot de miel permettant ainsi de réduire le niveau de vulnérabilité de l'entreprise. Nos principaux défis rencontrés ont été au niveau de la complexité de mise en œuvre et aussi dans l'acquisition du matériel sophistiqué pour pouvoir supporter la solution.

Mots clés : Détection et prévention d'intrusions, Détection distribuée, capteur, intrusion, honeynet, réseau informatique.

ABSTRACT

In this work, in order to increase the level of security of the IP-TELRA company which until now had only minimal computer and network security, not guaranteeing the best security of the company's data and resources. , we propose a distributed intrusion detection and prevention architecture based on the Bro network intrusion detection system (which has become Zeek since 2018), for large area networks in general and the IP-TELRA company network especially. The IP-TELRA company network offers several services, including the interconnection of certain structures in order to give them access to the Internet and certain resources. IP-TELRA must therefore have better security tools to continue to ensure a good quality of service. In the distributed intrusion detection and prevention architecture that we propose for this network, each entity communicates at the appropriate time with the other entities with a view to sharing important events. Also, we propose a network of honeypots (honeynet) for the study of the tools and behaviors of hackers to adapt our rules and security measures in order to make security within IP-TELRA even more robust. This honeypot network is built to replicate the production environment of the network in order to gather data on attacks that would target network servers. At the end of our investigation, we were able to set up an intrusion detection and prevention system using the bro intrusion prevention and detection system coupled with a honeypot network, thus reducing the level of vulnerability of the company. Our main challenges encountered were in terms of the complexity of implementation and also in the acquisition of sophisticated equipment to be able to support the solution.

Keywords: Intrusion detection and prevention, distributed detection, sensor, intrusion, honeynet, computer network.

LISTE DES FIGURES

LISTE DES TABLEAUX

ACRONYMES

AAFID : Autonomous Agents for Intrusion Detection.

ACL : Access Control List.

CSM : Cooperating Security Managers.

DIDMA : Distributed Intrusion Detection using Mobile Agents.

DIDS : Distributed Intrusion Detection System.

DMZ : Demilitarized Zone.

DNS : Domain Name Service.

DOS : Denial of Service.

DTK : Deception ToolKits.

FTP : File Transfer Protocol.

GrIDS : Graph-based Intrusion Detection System.

HIDS : Host based Intrusion Detection System.

HIPS : Host based Intrusion Prevention System.

HTML : HyperText Markup Language.

HTTP : HyperText Transfer Protocol.

HTTPS : Hyper-Text Transfer Protocol Secure.

ICMP : Internet Control Message Protocol.

IDS : Intrusion Detection System.

IDWG : Intrusion Detection Working Group.

INTERNET : Interconnected Network.

IP : Internet Protocol.

IPS : Intrusion Prevention System.

IRC : Internet Relay Chat.

ISO : International Standards Organization.

KIDS : Kernel Intrusion Detection System.

KIPS : Kernel Intrusion Prevention System.

LAN : Local Area Network.

LBNL : Lawrence Berkeley National Laboratory.

MAC : Medium Access Control.

MySQL : My Structured Query Language.

NIDS : Network Intrusion Detection System.

NIPS : Network Intrusion Prevention System.

NSM : Network Security Monitor.

OSI : Open System Interconnect.

PDU : Protocol Data Unit.

RFC : Request For Comment.

SNORT : The Open Source Network Intrusion Detection System.

SSH : Secure Shell.

SSL : Secure Socket Layer.

TCP : Transmission Control Protocol.

TELNET : Terminal Network.

TTL : Time To Live.

UDP : User Datagram Protocol.

VPN : Virtual Private Network.

WWW : World Wide Web.

INTRODUCTION

Les réseaux informatiques sont devenus des ressources vitales et déterministes pour le bon fonctionnement des entreprises. De plus, ces réseaux sont ouverts de fait qu'ils sont pour la plus parts raccordés à l'Internet [1]. Cette ouverture qui permet de faciliter la communication, engendre malheureusement des risques importants dans le domaine de la sécurité informatique. Des données récemment publiées par l'Agence nationale des TIC (ANTIC) révèlent des pertes financières de plus de 12 milliards de FCFA au Cameroun dues à la cybercriminalité en 2021, soit deux fois plus que l'année 2019 [2]. Les utilisateurs de l'Internet ne sont pas forcements pleins de bonnes intentions, ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour réaliser leurs attaques. Les conséquences de ces attaques peuvent être lourdes pour un particulier (pertes d'informations, ou pire encore vol d'informations, atteinte à la vie privée...) et pour une entreprise (perte du savoir-faire, atteinte à l'image de marque, perte financière...). Pour cela, les administrateurs déploient des solutions de sécurité efficace capable de protéger le réseau de l'entreprise.

Réduire ou éliminer les failles de sécurité d'un réseau afin de diminuer les risques de concrétisation de menaces est devenu un point important dans la mise en place des réseaux. Parmi les préceptes connus dans le domaine de la sécurité informatique, se trouve celui énonçant que pour une entreprise connectée à l'Internet, le problème aujourd'hui n'est plus de savoir si elle va se faire attaquer, mais quand cela va arriver [3]; une solution possible est alors d'essayer de repousser les risques dans le temps par la mise en œuvre de divers moyens destinés à augmenter le niveau de sécurité du réseau. Il est ainsi nécessaire de disposer d'outils spécialisés dont le rôle sera de surveiller les données qui transitent sur un système et de réagir si certaines semblent suspectes. Les logiciels qui sont les plus à même d'effectuer cette tâche sont les systèmes de détection et de prévention d'intrusions. A notre arrivé au sein de l'entreprise IP-TELRA ce type de système n'existait pas, mettant ainsi l'entreprise dans un état de vulnérabilité permanente face aux attaques bien que celle-ci dispose d'un niveau de sécurité minimale mais ne garantissant pas au mieux la sécurité des données et des entités de son réseau interne en vue de l'importance et de la criticité de celles-ci. Heureusement jusqu'ici nous

n'avons pas encore connu le pire au sein d'IP-TELRA mais pour une entreprise en pleine croissance comme tel et dans la mesure d'une sécurité préventive plus accentué car nous comptons dans les statistiques Camerounais plus de 12000 attaques des entreprises entre 2013 et 2017 qui ne cesse d'augmenter d'année en année [2] [4]. L'objectif principal qui nous guide dans ce travail est de proposer une architecture distribuée de détection et de prévention d'intrusions basée sur l'utilisation de systèmes de détection d'intrusions. Nous proposons également un réseau de pots de miel dont le but est d'étudier les menaces contre IP-TELRA, afin de chaque fois réadapter la politique implémentée dans les systèmes de détection contre les nouvelles tendances de menaces. Pour arriver a bien dans notre travail nous devrons, Installer Bro IDS pour le filtrage des paquets, Créer des règles de filtrage pour sécuriser de réseau, Installer un ordinateur pot de miel pour tromper les attaquants, Faire communiquer les différents équipements dans le réseau, Mettre en place un réseau d'IDS distribué. Nous proposons dans ce projet, une approche d'architecture distribuée de détection et de prévention d'intrusions basée sur l'utilisation de système de détection d'intrusions. Également, nous proposons un espace d'étude des mécanismes d'attaque, basé sur les pots de miel. La combinaison de ces deux moyens permettra d'offrir un environnement de surveillance un peu plus fiable au réseau de l'entreprise IP-TELRA.

Pour atteindre les objectifs de notre travail, nous allons dans un premier temps traiter de l'état de l'art qui se subdivise en deux chapitres. Le premier nous renseignant sur la sécurité et l'existant d'IP-TELRA et le second chapitre nous donne un enseignement sur le concept des IDS, des pots de miel et des capteurs distribués. Dans un second temps nous allons traiter de l'analyse et la mise en œuvre de la solution elle se subdivisé en trois chapitres, le chapitre premier traitant de l'analyse de la solution ; Le second chapitre présente le cahier de charge utile à la réalisation de notre projet ; Enfin le dernier chapitre ressort à travers une méthodologie, une mise en œuvre et présente également les résultats.

PARTIE 1 :

État de l'Art

Dans cette partie nous présenterons successivement les notions de sécurité informatique, l'existant de l'entreprise IP-TELRA et enfin les différents travaux effectués dans ces différents domaines.

Chapitre 1 : La sécurité informatique

Dans ce chapitre, nous définissons tout d'abord la notion de sécurité informatique, nous présentons son importance dans une organisation ainsi que quelques mécanismes de sécurité existant pour contrecarrer les menaces connues. Ensuite nous parlerons de l'existant d'IP-TELRA ainsi que les défaillances de celui-ci point de vue sécurité informatique.

1 La sécurité informatique

Le système d'information est généralement défini par l'ensemble des données, des ressources matérielles, logicielles, humaine et procédure de l'entreprise permettant de collecter, stocker, traiter et diffuser l'information. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger [5]. La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu et par des personnes autorisées.

Les exigences fondamentales de la sécurité Informatiques se résument à assurer :

- **La disponibilité :** La disponibilité est la caractéristique d'une information d'être accessible et utilisable par son destinataire autorisé à l'endroit et à l'heure prévue.
- **La confidentialité :** La confidentialité vise à empêcher tout accès non autorisé à des informations sensibles.
- **L'Intégrité :** L'intégrité des données est l'exactitude, l'exhaustivité et la cohérence globales des données.

Figure 1: Les principes de la sécurité informatique [6]

Tout au long de ce chapitre, nous présenterons les enjeux de ce dernier, les principales menaces pesant sur la sécurité des réseaux, le cycle de vie d'une cyberattaque ainsi que les mécanismes de défense.

1.1 Sécurité des réseaux

La sécurité d'un réseau est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir sa sécurité. En général, la sécurité d'un réseau englobe celle du système informatique sur lequel il s'appuie. À un niveau fondamental, la sécurité du réseau est l'opération qui consiste à protéger les données, les applications, les appareils et les systèmes qui sont connectés au réseau.

1.2 Importance de la sécurité des réseaux

1.2.1 Les enjeux

1.2.1.1 Enjeux économiques

Les organismes ou entreprises à but lucratif on presque toujours la même finalité : c'est de réaliser des bénéfices sur l'ensemble de leurs activités. Cette réalisation est rendue possible grâce à son système d'information considéré comme moteur de développement de l'entreprise. D'où la nécessité de garantir la sécurité de ce dernier. La concurrence fait que des entreprises s'investissent de plus en plus dans la sécurisation de leurs systèmes d'information et dans la qualité de service fournit aux clients.

1.2.1.2 Enjeux politiques

La plupart des entreprises ou organisations se réfèrent aux documents officiels de sécurité élaborés et recommandés par l'État. Ces documents contiennent généralement des directives qui doivent être appliquées par toute structure engagée dans un processus de sécurisation du réseau. Dans le cadre du chiffrement des données par exemple, chaque État définit des cadres et mesures d'utilisation des algorithmes de chiffrement et les recommande aux entreprises exerçant sur son territoire. Le non- respect de ces mesures et recommandations peut avoir des conséquences graves sur l'entreprise. A ce niveau, l'enjeu est plus politique parce que chaque État souhaite être capable de décrypter toutes les informations circulant dans son espace.

1.2.1.3 Enjeux juridiques

Dans un réseau, on retrouve de l'information multiforme (numérique, papier, etc.). Le traitement de celle-ci doit se faire dans un cadre bien définit et dans le strict respect des lois en vigueur. En matière de juridiction, le non-respect des lois et exigences relatives à la manipulation des informations dans un système d'information peut avoir des conséquences graves sur l'entreprise. A l'instar de la protection des données en général, la sécurisation des traitements doit trouver un équilibre entre, d'une part, les droits des personnes concernées par les traitements de données et, d'autre part, les intérêts des personnes traitant ces données

1.2.2 Les vulnérabilités

Dans le domaine de la sécurité informatique, une vulnérabilité ou faille est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient. Ces vulnérabilités sont la conséquence de faiblesses dans la conception, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système, mais il s'agit souvent d'anomalies logicielles liées à des erreurs de programmation ou à de mauvaises pratiques. Ces dysfonctionnements logiciels sont en général corrigés à mesure de leurs découvertes, mais l'utilisateur reste exposé à une éventuelle exploitation tant que le correctif (temporaire ou définitif) n'est pas publié et installé. Une telle exploitation peut causer des impacts importants. De nouvelles vulnérabilités sont découvertes régulièrement.

Il est possible de les regrouper en plusieurs familles :

1.2.2.1 Vulnérabilités humaines

L'être humain de par sa nature est vulnérable. La plupart des vulnérabilités humaines proviennent des erreurs (négligence, manque de compétences, surexploitation, etc.), car l'être humain est imparfait et est soumis à des erreur. Ne dit-on pas souvent que l'erreur est humaine ? Un SI étant composé des humains, il convient d'assurer leur sécurité si l'on veut garantir un maximum de sécurité dans le SI.

1.2.2.2 Vulnérabilités techniques

Avec la progression exponentielle des outils informatiques, les vulnérabilités technologiques sont découvertes tous les jours. Ces vulnérabilités sont à la base dues à une négligence humaine lors de la conception et la réalisation. Pour être informé régulièrement des

vulnérabilités technologiques découvertes, On peut commencer par s'inscrire sur une liste ou des listes de diffusion mises en place par les CERT (Computer Emergency Readiness ou Response Team).

1.2.2.3 Vulnérabilités physiques

Les vulnérabilités d'ordre organisationnel sont dues à l'absence des documents cadres et formels, des procédures (de travail, de validation) suffisamment détaillées pour faire face aux problèmes de sécurité du système. Quand bien même ces documents et procédures existent, leur vérification et mises à jour ne sont pas toujours bien assurées.

1.2.3 Les menaces

Figure 2: Contexte de menaces [7]

Les menaces informatiques sont variées et redoutables d'efficacité. Toutes les études arrivent à la même conclusion : les entreprises sont de plus en plus victimes de piratage informatique. Voici des différentes menaces auxquelles sont confrontées les entreprises.

1.2.3.1 Les logiciels de rançon (Ransomwares)

Il s’agit des virus les plus répandus actuellement. C’est la version numérique du racket : les données de l’entreprise sont prises en otage par un pirate. Le principe de cette infection est le suivant : caché dans une pièce jointe, un programme malveillant chiffre les documents stockés dans l’ordinateur qui a été le premier infecté. Mais en quelques secondes, tous les

fichiers partagés par les différents collaborateurs sont également bloqués. Impossible de les ouvrir, sauf si l'on paie une rançon dont le montant qui augmente au fil du temps pour faire monter la pression.

La figure ci-dessous montre l'interface du logiciel (virus) « WannaCry »de type Ransomware

Figure 3: Interface de WannaCry

1.2.3.2 Hameçonnage (Phishing / Scamming)

Un autre danger fait toujours parler de lui : le phishing ou l'hameçonnage. Tout le monde connaît ces emails usurpant l'identité d'une entreprise privée ou d'une administration. Mais les cybercriminels ont beaucoup d'imagination et de talents pour concevoir de faux courriers avec le logo officiel. On peut facilement tomber dans ce piège. Ce sont alors des mots de passe qui sont récupérés ou l'installation de programmes malveillants qui s'exécute alors avec le « consentement » de l'utilisateur. À ce jour, il s'agit de la technique la plus « rentable », selon la dernière étude de Google à ce sujet.

Figure 4: illustration du Phishing

1.2.3.3 La fuite de données

Elle peut être due à l'infiltration du réseau informatique par un pirate. Mais elle peut aussi provenir d'un salarié de l'entreprise ! Les employés constituent historiquement le plus grand risque. Ils ont des connaissances, des autorisations et le temps en leur faveur. Dès lors, la fuite de données peut être intentionnelle. Un employé enregistre des informations critiques sur une clé USB, ou les envoie sur sa messagerie personnelle, pour ensuite les revendre à la concurrence. Cette fuite de données peut être également due à la négligence des collaborateurs qui naviguent sur des sites non sécurisés ou laissent leur session ouverte ou utilise des mots de passe trop faible.

Figure 5: Illustration de la fuite de données

L'une des méthodes couramment utilisées par les pirates informatiques pour espionner le trafic sur le réseau Le Sniffing ou renifleur.

Un Sniffer est généralement utilisé pour intercepter les paquets qui circulent sur un réseau. Il offre, à cet effet, la possibilité pour un hacker d'examiner le contenu d'un certain nombre de paquets qui ne lui ont pas été initialement destinés. En tant que renifleur, cet outil peut donc intercepter tout type d'informations émises à travers le réseau et par conséquent afficher à la fois l'identité des utilisateurs au même titre que leurs mots de passe, surtout lorsque ces informations sont transférées par des protocoles qui ne sont pas suffisamment sécurisés comme : le FTP (File Transfert Protocol), la DNS (Domain Name System) ou encore le HTTP (Protocole de transfert hypertexte). Lorsque les données ne sont donc pas cryptées et qu'elles doivent passer à travers une interface réseau de l'ordinateur par l'intermédiaire duquel s'exécute le renifleur réseau ou sniffer, les informations sont immédiatement interceptées par cette machine sans la moindre difficulté. La figure suivante présente le fonctionnement de base d'une attaque.

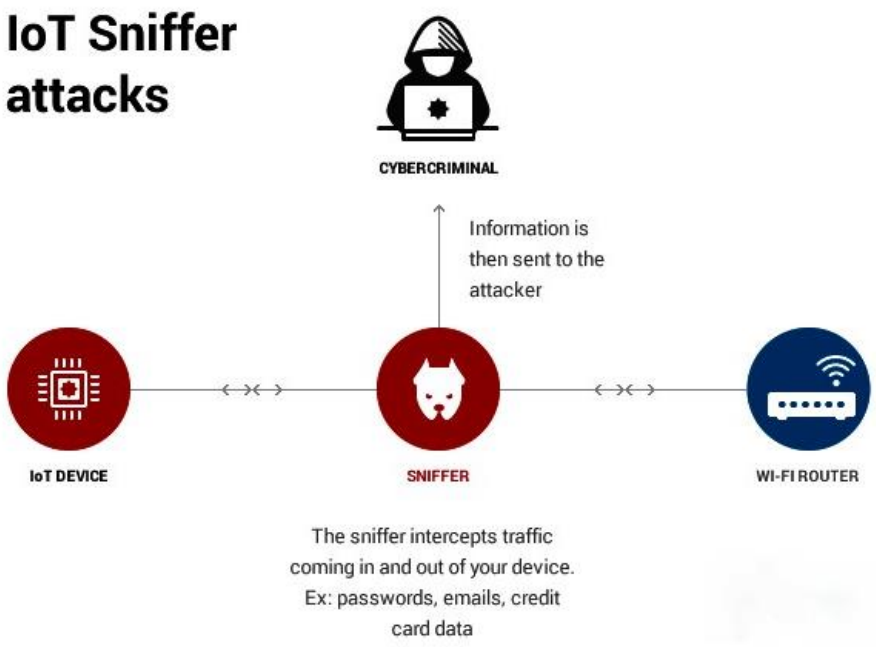


Figure 6 : Attaque par sniffing

1.2.3.4 Les attaques par Déni de Service DDOS (Distributed Denial of Service attack)

L'attaque DDos va consister à demander à ce bataillon corrompu de se connecter ou d'envoyer des données en même temps vers une cible. Croulant sous les demandes de connexion ou inondée par des Gigabit/s de données, cette cible devient en quelques secondes inaccessible pour tous les internautes. Les pirates n'ont plus qu'à demander une rançon à

l'éditeur du site pour arrêter leur attaque ou en profitent pour traverser une barrière de protection saturée plus capable d'agir.

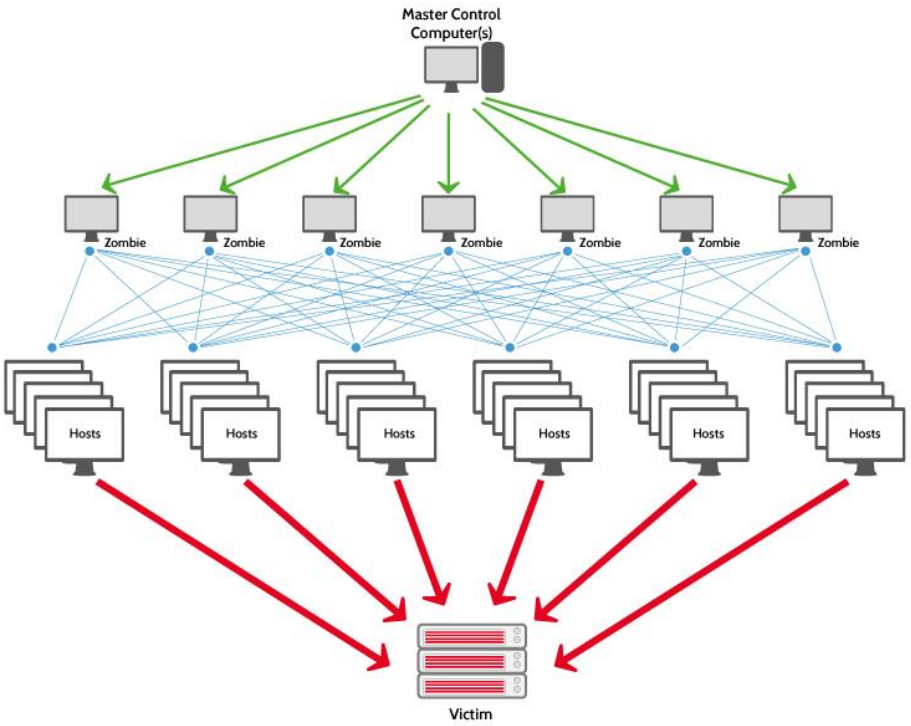


Figure 7: Attaque DDos

1.2.3.5 IP Spoofing

L'usurpation d'une adresse IP d'une machine est utilisé pour cacher sa véritable identité, et donc de se faire passer pour quelqu'un autre, le plus souvent une machine de confiance du réseau attaqué. Le principe de cette attaque consiste en la création des paquets IP en modifiant l'adresse IP Source. Cependant, d'autres mécanismes doivent être mis en place, sinon la réponse au paquet ne retournera pas à son émetteur, du fait de la falsification de l'adresse IP. De ce fait la réponse est retournée à la machine "spoofée". Cette technique peut être utile dans le cas d'authentification basée sur une adresse IP. Pour ce faire, il existe des utilitaires qui permettent de modifier les paquets IP ou de créer ses propres paquets tels que "hping2". Grâce à ces utilitaires, il est possible de spécifier une adresse IP différente de celle que l'on possède, et ainsi se faire passer pour une autre machine. La figure suivante nous montre un cas précis.

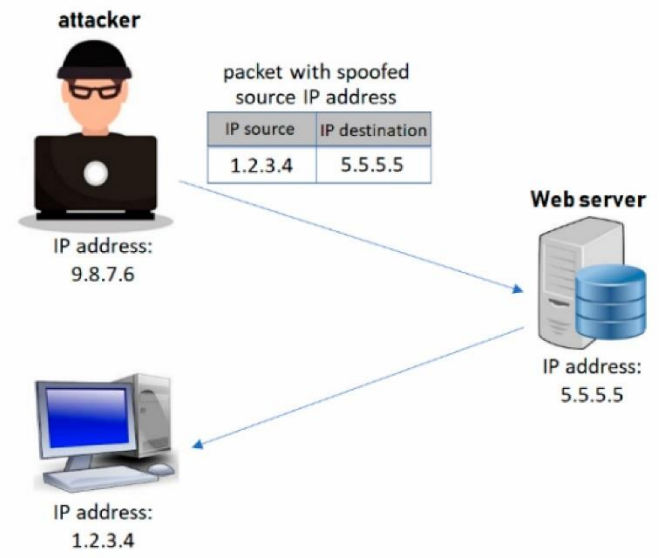


Figure 8: Attaque IP Spoofing

1.3 Statistique cybercriminalité au Cameroun

Les bandits du net ont porté un coup important à l'économie nationale l'année dernière via des techniques le plus souvent citées par les experts en termes de cyber risques en Afrique.

Le **scamming** et **l'hameçonnage** ont provoqué **6 milliards de pertes financières**, les violations des systèmes d'informations d'administrations ont emporté **2,5 milliards** et le **skimming** (détournement des informations bancaires au guichet automatique bancaire) a permis aux criminels de dérober **3,7 milliards de francs CFA**. En somme, **12,2 milliards de FCFA perdus** en une année contre 6 milliards en 2019 observe l'ANTIC [2].

L'Agence dénombre **27 052 vulnérabilités détectées en 2021** dans les systèmes de sécurité informatique des établissements publiques et privées au Cameroun. Elle observe également que l'usurpation d'identité est une infraction de plus en plus répandue sur les réseaux sociaux dans le pays. En 2019, plus de 5 500 faux comptes sur Facebook ont été utilisés par des cybercriminels pour arnaquer des citoyens non avertis ; 4063 ont été fermés, en collaboration avec le réseau social concerné [4].

Concernant l'état de la sécurité des applications en entreprise, en 2020 la fondation digitale Gefona consacrée au développement numérique en Afrique a relevé que 56,3% de la menace qui pèse sur les applications et les données des entreprises est due à des attaques d'applications Web et à une authentification frauduleuse.

16% des entreprises disposent d'un pare-feu d'application Web, parmi lesquelles seulement 8,4% effectuent des tests de pénétration alors que la majorité des entreprises se concentrent encore sur la sécurité au niveau du réseau, laissant leurs applications vulnérables aux attaques de piratage et à l'exploitation.

D'après la fondation, si les entreprises camerounaises sont conscientes des menaces de sécurité et des risques pour leurs systèmes en général, elles ne prêtent pas beaucoup d'attention à la sécurité au niveau des applications.

Selon la ministre camerounaise des postes et des télécommunications, **Minette Libom Li Likeng,** le Cameroun est aujourd'hui confronté à plusieurs défis liés à l'Internet, notamment les dispositions de sécurité pour prévenir et contrôler les risques technologiques majeurs [4].

Elle a déclaré lors d'un atelier autour de la lutte contre la cybercriminalité et la cyberdélinquance, le jeudi 3 mars 2022 que « ces menaces ne peuvent être pleinement prises en charge que par le développement d'une solide culture de cybersécurité, la création de capacités d'intervention robustes et l'adoption de politiques nationales appropriées et efficaces ».

1.4 Mécanismes de sécurité

Due à l'abondance des menaces, Il faut mettre en place des mécanismes pour s'assurer la confidentialité, l'intégrité et la disponibilité des services. A cet effet il existe une multitude de moyens pour réduire le niveau de menace d'un système.

Figure 9: Mécanisme de sécurité

Parmi les moyens de sécurité existant, nous pouvons citer :

1.4.1 Cryptage

Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Ce principe est généralement lié au principe d'accès conditionnel. Bien que le chiffrement puisse rendre secret le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre.

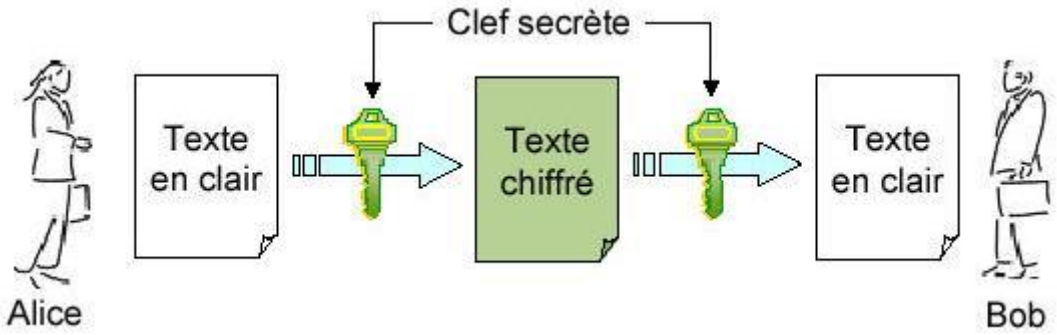


Figure 10: Chiffrage asymétrique

1.4.2 Le Pare-Feu

Un firewall (ou pare-feu) est un matériel ou un logiciel utilisé pour protéger un réseau local des intrusions extérieures. Il agit comme une barrière de protection et de sécurité empêchant la fuite de certaines informations en dehors du réseau informatique. Il permet de gérer, de contrôler, d'analyser, et de sécuriser le réseau de l'entreprise.

Lorsque l'on met en place un réseau informatique avec une multitude d'ordinateurs connectés à celui-ci, ces derniers risques potentiellement une attaque par un hacker informatique. L'objectif de cet hacker est donc d'infiltrer votre réseau et de détecter d'éventuelles failles de sécurité pour accéder à vos données. Mais la menace peut également venir de l'intérieur lorsqu'un utilisateur clique malencontreusement sur un lien contenant un virus.

Il est donc important pour les entreprises de protéger son réseau en installant un dispositif de pare-feu que ce soit pour le filtrage des données interne ou externe et c'est là

qu'intervient le firewall. Il va faire l'intermédiaire entre le réseau local (privé) et le réseau externe. Il va contrôler et filtrer les données échangées. Le fonctionnement d'un Firewall repose sur des règles prédéfinies pour autoriser (allow), bloquer (deny) ou rejeter (drop) la connexion.

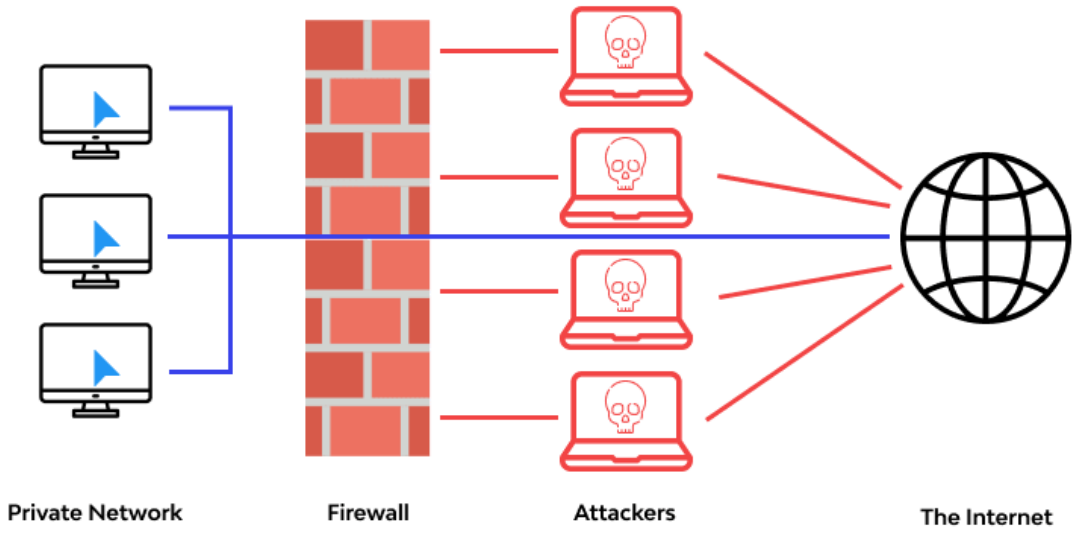


Figure 11: Fonctionnement d'un pare-feu

1.4.3 L'Antivirus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programmes modifiants ou supprimant des fichiers, que ce soit des documents de l'utilisateur de l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur.

Un antivirus vérifie les fichiers et courriers électroniques, les secteurs de boot (pour détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels Réseaux (dont internet), etc. nous avons un ensemble d'antivirus qualifié et disponible sur marché.

Figure 12: Quelques antivirus

1.4.4 VPN

Dans les réseaux informatiques, le réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une technique permettant aux postes distants de communiquer de manière sûre, tout en empruntant des infrastructures publiques (internet). Un VPN repose sur un protocole, appelé protocole de tunnellisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

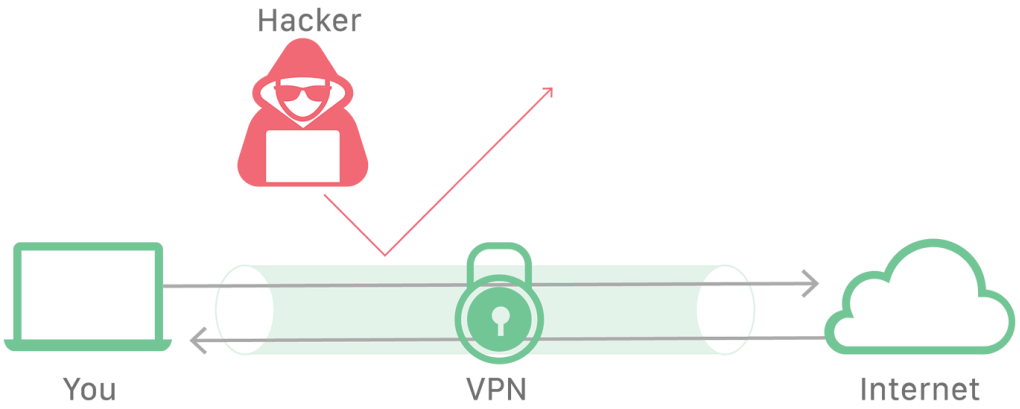


Figure 13: Fonctionnement VPN

1.4.5 IDS/IPS

Un système de détection d'intrusion est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée. Il permet ainsi d'avoir une connaissance sur les tentatives réussie comme échouées des intrusions.

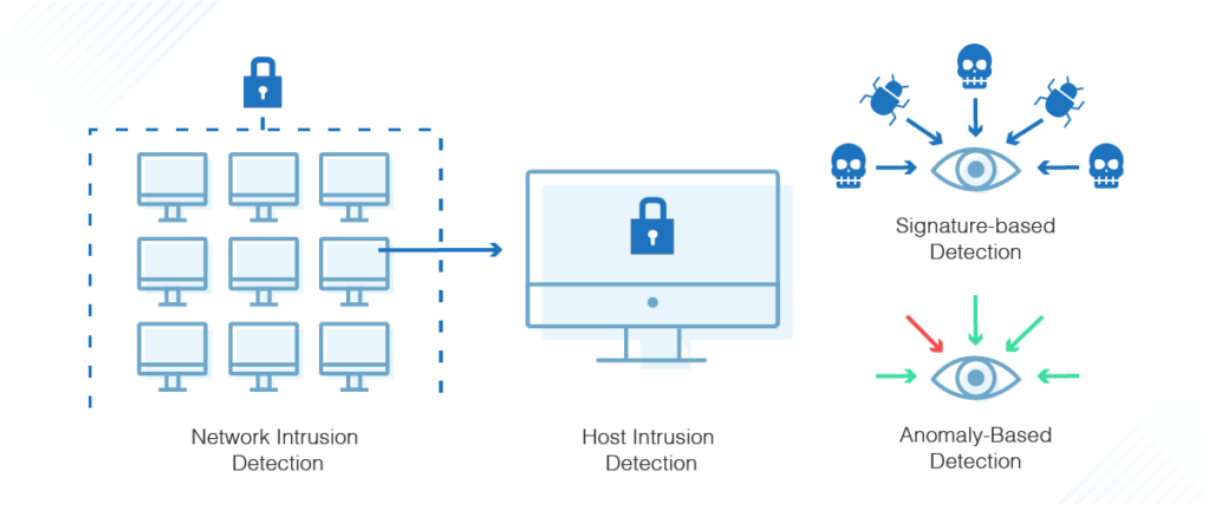


Figure 14: Protection IDS/IPS

1.4.6 Monitoring

Le monitoring ou monitorage est une activité de surveillance et de mesure d'une activité informatique. On l'emploie pour permettre la supervision.

Les raisons peuvent être variées :

- ✓ Mesure de performance, en termes de temps de réponse par exemple ;
- ✓ Mesure de disponibilité, indépendamment des performances ;
- ✓ Mesure d'intégrité, l'état des processus sur une machine Unix par exemple, ou bien qu'une page web n'a pas été modifiée (sécurité informatique) ;
- ✓ Mesure de changement, surveillance de sites de News avec Google Actualités.

Figure 15: Principe de monitoring

1.5 Cycle de vie d'une cyberattaque

Les attaquants utilisent des vecteurs d'infection. Vous connaissez peut-être certains d'entre eux : je veux parler du phishing, de l'exploitation de vulnérabilité ou encore des faiblesses de sécurité telles que l'utilisation de mots de passe faibles, ou l'exposition de serveurs sensibles.

Pour mieux expliquer le cycle d'attaque, je vous invite à regarder ce schéma extrait du Mitre (une organisation non lucrative proposant des référentiels en cybersécurité) représentant les actions d'un attaquant à chaque étape :

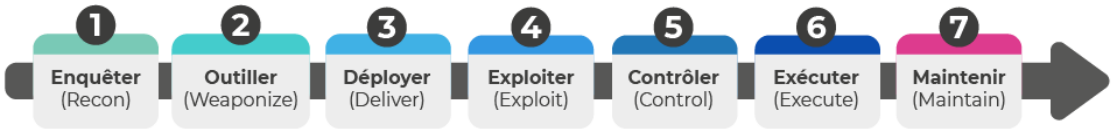


Figure 16: Cycle de vie d'un cyber attaque

Recon (Enquêter) : L'attaquant recherche des informations sur sa cible (employés, activités, projet…). Il peut également faire de la collecte d'information, qui sera utilisée pour les phases suivantes, telles que la recherche de vulnérabilité.

Weaponize (Outiller) : L'attaquant définit et prépare les outils nécessaires pour la compromission : campagne de phishing, préparation de code d'exploitation...

Deliver (Déployer): Puis, il déploie les attaques précédemment définies afin de compromettre les cibles. Les vecteurs d'infection sont utilisés lors de cette phase.

Exploit (Exploiter) : L'exploitation consiste ici à déployer les outils après la compromission initiale. L'attaquant pourra également effectuer des élévations de privilèges. À partir de cette étape, il faut que votre monitoring de la sécurité puisse détecter ses actions, car l'attaquant a la main sur votre réseau.

Control (Contrôler) : L'attaquant commence à prendre le contrôle des systèmes compromis, et effectue une reconnaissance interne de l'entreprise. On parle également de mouvements latéraux.

Execute (Exécuter) : Pendant l'exécution, l'attaquant met en place les actions finales, comme l'exfiltration de données sensibles.

Maintain (Maintenir) : Enfin, l'attaquant garde la main sur les systèmes en maintenant un accès distant au système compromis. N.B. : Un attaquant peut rester sur un réseau pendant plusieurs mois avant que vous le détectiez !

1.6 Les mythes des entreprises sur la cybersécurité et la cybercriminalité [7]

- **Mythe 1 : Ma compagnie est trop petite pour être ciblée par des hackers**

Les pirates informatiques considèrent les PME comme des proies faciles. Elles sont les victimes de la majorité des attaques (64%) justement parce qu'elles sont mal protégées.

Elles demeurent vulnérables aux menaces telles que des employés mécontents, la concurrence, l'ingénierie sociale, et la compromission de messagerie.

- **Mythe 2 : J'ai déjà un pare-feu, un antivirus, et une solution de sauvegarde. Ai-je vraiment besoin de plus ?**

Cet ensemble de solutions était certainement suffisant par le passé. Mais aujourd'hui, la majorité des cyberattaques sont suffisamment sophistiquées pour contourner les précautions de sécurité de base d'une entreprise. Ce qui a fonctionné hier ne suffit plus à protéger contre les menaces d'aujourd'hui. La sécurité doit être impérativement adaptée.

Et bien sûr, il est beaucoup plus économique de résoudre ce problème avant qu'il ne se produise, surtout en sachant que la violation moyenne coûte environ 200 000 $ à une PME, et cette somme est en augmentation complète.

- **Mythe 3 : Pourquoi un criminel voudrait-il mes données ? Elles ne sont pas si précieuses !**

En fait, vos données sont souvent plus précieuses que vous ne le pensez, lorsqu'elles sont vendues sur web clandestin. Votre concurrent principal paierait-il 10 000 $ pour vos plans d'affaires, vos plans d'acquisition ou votre stratégie marketing ? Est-ce que quelqu'un paierait pour vos noms d'utilisateur et mots de passe, afin qu'il puisse se connecter à votre réseau à votre insu ? Très probablement. C'est souvent le cas avec les comptes de réseaux sociaux de certains utilisateurs.

De plus, dans le cas des ransomwares, le criminel sait que vous avez besoin de vos données pour fonctionner et que vous paierez pour obtenir la clé de déchiffrement.

- **Mythe 4 : Je suis déjà couvert avec mon contrat de services gérés.**

Lorsque vous avez souscrit votre contrat de services gérés, votre fournisseur a certainement inclus les meilleurs outils pour vous gérer votre réseau, et apporter une sécurité de base.

Le problème est que les cybercriminels ont amélioré leurs compétences et attaquent maintenant d'une manière qui n'est pas couverte par les outils en place. Et bien que vous ayez toujours besoin de la couverture actuelle, vous devez envisager d'autres protections qui sont absolument nécessaires aujourd'hui pour vous protéger de manière adéquate.

- **Mythe 5 : Je suis couvert par ma cyber assurance.**

L'objectif de la cyber assurance est de transférer une partie du risque associé à une faille de sécurité à l'assureur. Mais la réalité est que le fait de souscrire cette assurance ne dispense

pas le client de disposer d'une sécurité adéquate. En effet même si la cyber assurance peut être utile, elle n'est pas un substitut à la mise en place et au maintien de politiques de sécurité et de formation appropriées.

Les compagnies d'assurance ne paieront pas si les entreprises ne peuvent pas prouver qu'elles ont mis en œuvre les moyens requis pour protéger leurs environnements contre les menaces de cybersécurité. Il est important de faire une distinction entre ce qui est évitable et ce qui échappe au contrôle de l'entreprise.

1.7 Gestion de risque

Partons d'un constat indiscutable

Menace + Vulnérabilités = Risque (le potentiel de perte ou de dommage lorsqu'une menace exploite une vulnérabilité)

Considérons l'ampleur de la menace

Les enquêtes récentes révèlent que plus de 80% des PME craignent d'être victimes d'une cyberattaque, et à juste titre. Selon Cyber Security Ventures en 2021 [7] :

- Près de la moitié de toutes les cyberattaques sont commises contre des PME.
- Toutes les 11 secondes, une entreprise sera victime d'un ransomware.
- Les cyberattaques par ransomware coûteront aux entreprises plus de 20 milliards de dollars.

1.8 Les normes sur la sécurité informatique [8]

ISO/IEC 27000:2018 offre une vue d'ensemble des systèmes de management de la sécurité de l'information (SMSI). Il comprend également les termes et définitions d'usage courant dans la famille de normes du SMSI. Le présent document est applicable à tous les types et à toutes les tailles d'organismes (par exemple : les entreprises commerciales, les organismes publics, les organismes à but non lucratif).

ISO/IEC 27001 est la norme la plus connue de la famille **ISO/IEC 27000:2018** qui n'en compte pas moins d'une douzaine. Elle spécifie les exigences relatives aux systèmes de management de la sécurité des informations **(SMSI)**. La mise en œuvre des normes de cette

famille par tout type d'organisation facilite le management de la sécurité d'actifs sensibles tels que les données financières, les documents de propriété intellectuelle, les données relatives au personnel ou les informations confiées par des tiers.

ISO/IEC 27039:2015 fournit des lignes directrices pour aider les organisations à se préparer au déploiement de systèmes de détection et de prévention des intrusions (IDPS). En particulier, il traite de la sélection, du déploiement et des opérations de l'IDPS. Il fournit également des informations de base à partir desquelles ces lignes directrices sont dérivées.

1.9 Etude de l'existant

L'analyse de l'existant permet de comprendre la nature du système actuel, décrit la solution présente du domaine d'étude au terme d'organisation. Le but de l'analyse de l'existant est la recherche des points forts et des points faibles du système existant. Ainsi, l'analyse de l'existant fait l'état de lieux du système actuel.

1.9.1 Présentation de l'architecture réseau existante

L'architecture réseau existant à ce jour à IP-TELRA se présente comme suit :

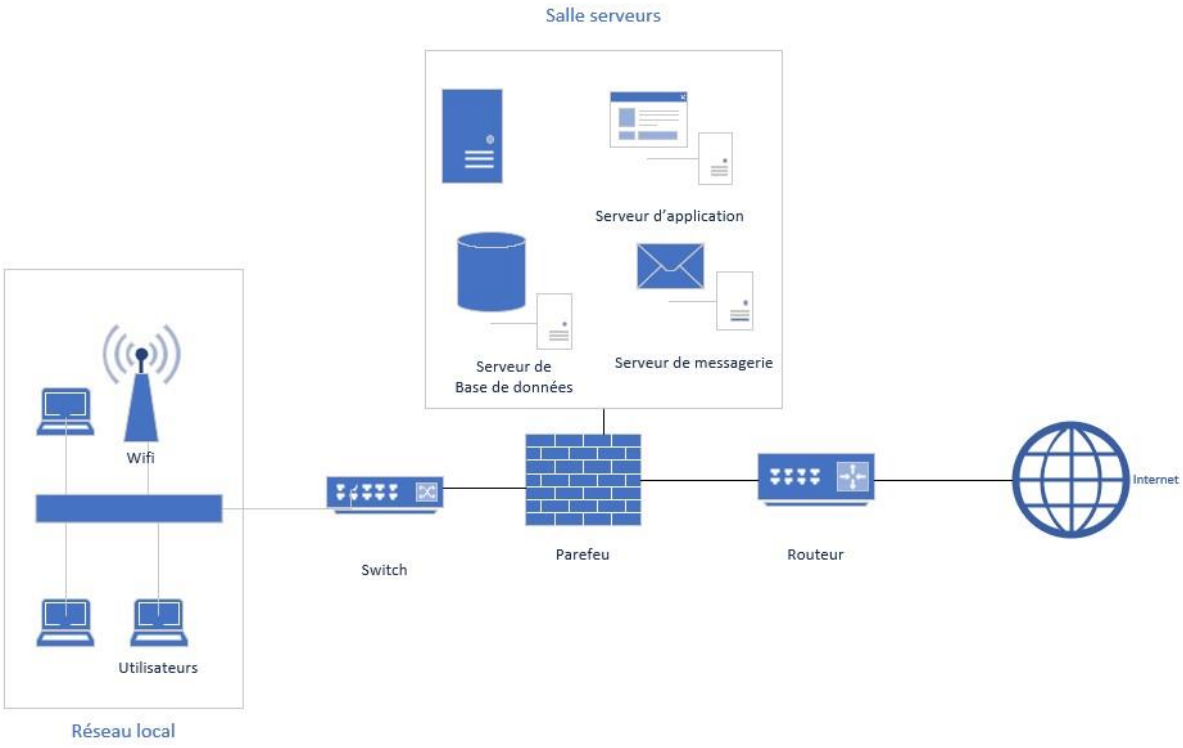


Figure 17: Architecture existante IP-TELRA

1.9.2 Etude des moyens de traitement des informations

1.9.2.1 Moyens matériels

L'entreprise dispose en son sein d'un grand nombre d'ordinateur, un serveur dédié, des imprimantes, des onduleurs, des stabilisateurs et d'outils disponible pour le réseau (Switch, routeur). Les principaux outils informatiques de la structure sont listés dans le tableau suivant :

Tableau 1: Moyen matériel d'IP-TELRA

Equipements	Nombre	Model	Usage
Routeur	01	Cisco 1921	Gérer le réseau et les connexions
Modem internet	01	Modem Camtel Huawei Hg8245	Accès à internet
Pare-feu	01	Cisco ASA 5505	Contrôle le trafic réseau entrant et sortant
Serveur	04	Serveur tour DELL PowerEdge T430	Stockage des données et des services
Switch	02	Cisco Catalyst 2960	Filtrage et connectivité des postes
Ordinateur fixe	08	DELL Optiplex 790 core i5 8Go ram	Permet aux employer d'effectuer leurs travaux en interne
Ordinateur portable	06	Dell E5450 i5-5300U -8Go ram	Permet aux employer d'effectuer leurs travaux en déplacement
Point d'accès wifi	03	TP-Link TL-WR740N	Donner un accès wifi au utilisateurs
Photocopieur	01	Canon IR Advance C5535i	Permet d'effectuer les taches d'impression et de photocopie

1.9.2.2 Moyens logiciels

L'entreprise dispose également d'un ensemble de moyen logiciel dans l'accomplissement de ces fonctions. Les logiciels principalement utilisés au sein de la structure sont listés dans le tableau ci-après :

Tableau 2: Moyen logiciel IP-TELRA

Logiciels	Version	Utilité
Logiciels Système		
Windows 10	10 21H2 Professionnelle (Octobre 2021)	Système d'exploitation pour les postes utilisateur
Ubuntu	20.04 23 avril 2020	Système serveur pour les sauvegardes et les réplications
Windows server 2016	1607 (10.0.14393.2363) (10 juillet 2018)	Pour la gestion des postes utilisations, les configurations et prise en charge de certains services et ressources.
Logiciels Applicative		
Microsoft office 2019	2206 (16.0.15330.20246) / 12 Juillet, 2022	Pour les éventuelles saisies, traitement de texte, tableur, note, etc.
Microsoft 365	Version 2208 (Build 15601.20148)	Pour les éventuelles saisies, traitement de texte, tableur, note, etc.
SQL Server 2012	11.0.2100.60 23/04/2021	Pour la gestion de base de données
VS Code	2019 v16.11.6	Pour la conception des sites et des applications
Teams Windows	12.0 (7/28/2021) 6sept. 2022	Pour les réunions en ligne et les échanges
Android-studio-2020	2021.2.1 (Chipmunk) / 9 Mai 2022	Pour la conception des applications Android
Antivirus Kaspersky Total Security	21.3. 10.391 18 juil. 2022	Pour la protection des postes contre les virus informatique

HTML, CSS, JavaScript, JAVA, LARAVEL, C++	/	Comme langage de programmation.

1.9.2.3 Moyens humains

Le service informatique de la direction générale du Groupe IP-TELRA est composé d'un informaticien qualifié, apte et dynamique capable d'assumer avec tant de dévouement les missions qui lui est assignées.

Le but du critique de l'existant est de recenser les points forts et faibles du système en cours ; Dans ce cas, l'analyste procède à une critique objective du système en cours.

1.10 Les points fort du système existant

Dans cette section nous soulevons les points forts dans l'organisation, l'architecture et la sécurité de la structure d'IP-TELRA.

Du point de vue moyen humain : La direction générale du Groupe IP-TELRA regorge en son sein un personnel qualifié et dynamique pour assurer la plupart de ces fonctions ;

Du point du système d'information : Il est utile de préciser que cela est encourageant de constater qu'au sein de la direction générale du Groupe IP-TELRA, les postes de travail sont opérationnels et occupés par un personnel apte à effectuer le travail au poste auquel il est affecté.

Du point de vue technique : nous notons la présence d'un serveur de réplication et de sauvegarde afin de garantir la disponibilité des données en cas de sinistre ainsi qu'un système de continuité d'énergie en cas de panne électrique.

Du point de vue maintenance : l'équipe de maintenance système assure les mises à jour régulières et correctives en termes de sécurité pour la totalité des systèmes d'exploitation et logiciels.

Du point de vue contrôle d'accès : l'administrateur adapte la politique de blocage de lecteur USB et le filtrage d'accès depuis et vers le réseau internet pour éviter le risque de propagation des virus.

Du point de vue sécurité : Chaque poste de travail dispose d'un antivirus Kaspersky à jour. L'architecture est protégée par un pare feu physique Cisco situé à l'entrée du réseau, il filtre le trafic venant de l'extérieur du réseau afin de détecter d'éventuelles menaces.

1.11 Les points faibles du système existant

Dans cette section nous soulevons les manquements à la sécurité dans l'architecture, les solutions et la politique de sécurité d'IP-TELRA.

Le premier manquement à la sécurité ici et qui présente un intérêt particulier pour nous est l'absence d'un système de sécurité robuste pour faire face aux éventuelles attaques des pirates informatique. Ils se limite ici juste à une sécurité assez minimale et basique qui est largement insuffisant quant' à l'importance des données à sécuriser.

Nous notons par ailleurs d'autres manquement à la sécurité répertorié ici par degré de criticité croissant à savoir :

Tableau 3: Point faible du système existant

Danger	Risque	Seuil de criticité
La lenteur dans la transmission des données au sein de la hiérarchie de l'entreprise.	Lenteur dans les transmissions et les prises de décision en cas de sinistre.	
Absence d'un guide de procédure.	Mauvaise reprise des activités en cas de sinistre. Lenteur dans l'exécution des taches.	
Absence d'une politique de sécurité.	Menace non détectée, pas d'évaluation de risques et pas de plan de reprise d'activité.	
Audit de sécurité non effectué au sein de la structure depuis sa création	Détermination des points faibles afin de pouvoir y remédier, non respects des normes	
L'insuffisance des informaticiens pour les multiples taches qui y sont effectuées.	Surcharge dans le travail qui conduit à la baisse de la productivité.	

Absence d'une politique sur le renforcement des mots de passe.	Vol de mots de passe, usurpation d'identité, vol d'informations	
L'absence d'un système de monitoring.	Interruption d'activité par suite d'une défaillance du matériel ou du logiciel	
L'absence d'un système de détection d'intrusion dans le réseau et d'un moyen d'anticiper sur les menaces liées à l'accès des données via internet.	Attaques de pirate informatique, pertes d'information et de données sensibles, pertes financières.	
L'absence d'une équipe dédiée à la veille, au monitoring de la sécurité et à l'investigation sur les incidents de sécurité.	Piratage du réseau, intrusions d'un agent malveillant au réseau, pertes d'informations et pertes financières.	

Description	Code de couleur
Danger immédiat	
Risque élevé	
Risque moyen	
Faible risque	
Très faible risque	

Figure 18: Code couleur des risques [9]

1.12 Quelques propositions de solution

En réponse à l'ensemble des menaces observé au sein de la structure, nous proposons un ensemble de solution [8]

Figure 19: Solution de sécurisation d'un système informatique

Conclusion partielle

Au terme du parcours des divers aspects de la sécurité des systèmes d'information, nous pouvons dire qu'en ce domaine prévenir est impératif, attendre de subir un sinistre pour prendre de mesures de correction est très souvent très tard et irréversible. Lorsqu'un accident ou un

pirate a détruit les données de l'entreprise et que celle-ci n'a ni sauvegarde ni site de secours, elle est condamnée, tout simplement. Nous avons également fait un état de l'existant de l'entreprise IP-TELRA et nous avons ressorti par cet effet les force et les faiblesses de celui en fin de trouver la mesure qui convient la mieux pour la sécurisation de son système

Dans le chapitre suivant, nous aborderons la détection et prévention d'intrusion ainsi que les pots de miel et la détection distribué d'intrusion.

Chapitre 2 : Les travaux sur les DIDS et Honeypot

Dans ce chapitre, nous allons un peu plus nous attarder sur les notions de détection et prévention d'intrusion ainsi que sur les pots de miel et la détection distribué d'intrusion. Tour a tour nous parcourrons leurs historiques, leurs architectures, leurs modes de fonctionnement ainsi que leurs revu de littérature.

2 Les travaux sur les DIDS et Honeypot

2.1 Détection et prévention d'intrusion

Les systèmes de détection et de prévention d'intrusions sont utilisés dans un réseau pour détecter les attaques externes ou internes. Nous présentons une analyse détaillée de ces systèmes, en mettant en évidence leurs forces et faiblesses pour la protection des systèmes informatiques [11].

2.1.1 Intrusion

De façon générale, une intrusion est un accès non autorisé à une ressource, une société, un groupe ou un système d'information. En informatique, elle désigne toute activité qui viole la politique de sécurité d'un système ou qui essaie de prendre en défaut le mécanisme de sécurité d'une organisation. C'est toute tentative réussie ou non d'exploitation de vulnérabilités, de failles de sécurité. Elle peut être exécutée depuis l'intérieur du réseau ou par des individus situés à l'extérieur et qui tentent de passer au travers des mécanismes de sécurité mis en place.

2.1.2 Détection et prévention d'intrusions

Un système de détection d'intrusions ou IDS est un outil logiciel destiné à repérer des activités anormales ou suspectes sur un système (un réseau ou un hôte).

C'est un outil qui essaie d'identifier toute introduction illégale ou tout comportement anormal sur un système d'information. Il est un ensemble de composants logiciels et matériels dont la fonction principale est de détecter et d'analyser toute tentative d'effraction au sein du système.

Lorsque la détection est suivie de solutions actives, alors on parle de système de prévention d'intrusions. Le principal avantage des IDS/IPS par rapport à tout autre système tel que les pares-feux est leur capacité à accéder aux contenus même des paquets et les analyser. La détection ne porte donc plus seulement sur les en-têtes de protocoles comme c'est le cas pour les pares-feux. Dans la suite de ce développement, le thème IDS sera utilisé pour se référer aux deux catégories et toute distinction particulière sera clairement exposée.

2.1.3 Historique

La détection d'intrusions tire ses origines des systèmes d'audit. L'objectif était d'automatiser l'audit des systèmes que jusqu'alors était fait manuellement par les administrateurs réseaux. Il s'agit bien, théoriquement, de détecter de manière automatique les violations de politique de sécurité ou de droit, qu'on appelle intrusions. Les premiers systèmes de détection d'intrusions ont été initiés par l'armée américaine qui publia dans les années 1970 les objectifs d'un système de sécurité, parmi lesquels figure la détection de toute tentative de violation de mécanisme de protection. Les premiers travaux ont réellement débuté avec J.P. Anderson en 1980 qui décrit dans une publication comment améliorer les mécanismes de sécurité. Se servant de ces travaux, Dorothy Denning et Peter Neumann proposèrent en 1987 un modèle théorique d'un système de détection d'intrusions. Vers la fin des années 1980, Todd Heberlein introduit l'idée de la détection d'intrusion réseau. Il développa en 1990 le NSM (Network Security Monitor) qui était le premier système de détection d'intrusions réseau. En 1992, U.S. Air Force, UC Davis et d'autres ont développé le concept du système de détection d'intrusion distribué (DIDS pour Distributed Intrusion Detection System), puis ont introduit l'approche hybride de la détection d'intrusions. [11]

2.1.4 Architecture interne d'un IDS [9]

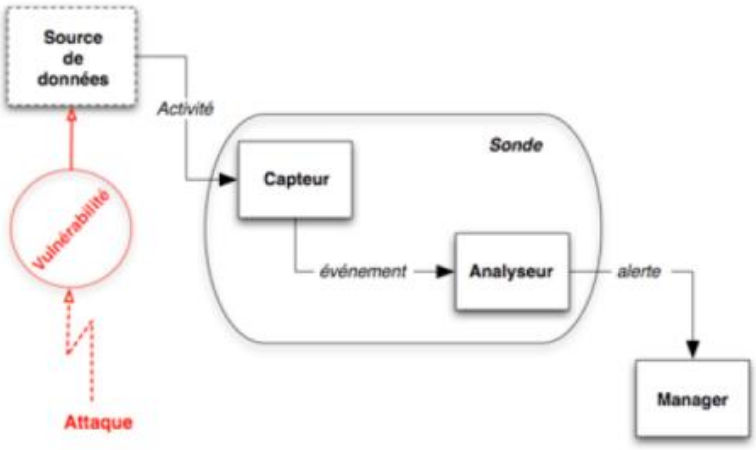


Figure 20 : Architecture d'un système de détection d'intrusions selon l'IDWG

L'architecture d'un système de détection d'intrusions dispose de trois composants communs à la majorité des IDS. Selon le modèle proposé par IDWG (Intrusion Detection

Working Group) Le capteur reçoit les données sources brutes c'est-à-dire les paquets réseau et les données d'audit. Il envoie ensuite des événements à l'endroit de l'analyseur. Ce dernier vérifie si certains événements sont caractéristiques d'activités malveillantes, auquel cas il génère des alertes qu'il envoie au manager. Ce dernier se charge de présenter les alertes à l'opérateur puis décide éventuellement de la réaction à adopter.

2.1.4.1 Le capteur

Le capteur est l'outil utilisé pour enregistrer les données brutes. Il est responsable de la collecte des données depuis le système surveillé. C'est le premier composant de la chaîne de détection à entrer en activité. Il permet donc de disposer des informations à analyser. Un pré-traitement peut être effectué sur les données à ce niveau notamment le filtrage pour éliminer les données non pertinentes ; ce qui permet de réduire la quantité de données à analyser par la suite. Il présente ensuite ces données sous forme d'événements à l'analyseur.

On distingue 3 types de capteurs en fonction des sources de données qu'ils utilisent :

- Les capteurs systèmes qui utilisent les données provenues des journaux d'audit des systèmes d'exploitation des machines et des appels systèmes effectués par les applications ;
- Les capteurs réseau qui écoutent les communications entre les différentes machines du réseau à travers une interface spécifique ;
- Les capteurs applicatifs qui se chargent d'enregistrer les données produites par les applications elles-mêmes. Ceci permet de suivre le fonctionnement d'une application spécifique.

2.1.4.2 L'analyseur

L'analyseur a pour objectif principal d'analyser le flux d'événements envoyé par le capteur pour identifier des données caractéristiques d'activités malveillantes. Il utilise alors ces événements afin de déceler une possible intrusion et génère en conséquence des alertes. Ces alertes sont ensuite présentées au manager.

2.1.4.3 Le manager

Le manager a pour rôle de traiter les alertes fournies par l'analyseur puis de les présenter à l'administrateur. Une corrélation d'alertes est nécessaire dans le cas de plusieurs sources d'alerte. Il peut également déclencher des mesures de traitement comme les actions suivantes :

- Confinement de l'attaque qui a pour but de limiter les effets possibles ;
- Éradication de l'attaque qui tente de l'arrêter ;
- Recouvrement qui est l'étape de restauration du système dans un état sain ;
- Diagnostic qui est la phase d'identification du problème, de ses causes et qui peut éventuellement être suivi d'actions contre l'attaquant (fonction de réaction).

Du fait du manque de fiabilité des systèmes de détection d'intrusions actuels, les réactions sont rarement automatisées, car elles peuvent se traduire par un déni de service en cas de réaction à des faux positifs.

2.1.5 Terminologie relative aux systèmes de détection d'intrusions

2.1.5.1 Faux Positif

Fausse alerte levée par le système de détection d'intrusions. C'est une alerte provenant d'un IDS et qui ne correspond pas à une attaque réelle. L'idéal est de ne pas avoir ce type d'alarme. Comme conséquence néfaste, lorsque l'administrateur de sécurité est inondé par ce type d'alerte, cela constitue une source d'ennui et l'amène parfois à ignorer des alertes réelles. De plus, cela peut entraîner une paralysie du réseau surtout dans le cas des IPS.

2.1.5.2 Vrai positif

Cela se réfère à une alarme où le système de détection d'intrusion reporte une intrusion réelle. Cela signifie qu'un système est entrain d'être compromis. Idéalement toutes les attaques devraient être détectées.

2.1.5.3 Faux négatif

Attaque non repérée par le système de détection d'intrusions. C'est une intrusion réelle qui n'a pas été détectée. Ceci est un comportement indésirable du système de détection d'intrusion pouvant avoir plusieurs origines.

Un IDS mal positionné privé d'une partie du trafic qu'il devrait analyser peut omettre des attaques. Aussi, cela pourrait être le cas lorsqu'il ne peut supporter le taux de trafic du réseau ; des paquets sont donc perdus.

Les signatures d'attaques ne sont souvent pas assez génériques ou comportent moins d'informations pour permettre la détection des variantes d'une attaque. Par ailleurs, il y a peu

de chance de détecter les attaques non publiées c'est-à-dire les attaques exploitant les vulnérabilités non encore découvertes.

2.1.5.4 Vrai négatif

Ce terme est utilisé pour décrire le cas où le système de détection d'intrusions trouve qu'un paquet est inoffensif et que cela est vrai.

2.1.5.5 Evasion

C'est une technique utilisée pour dissimuler une attaque et faire en sorte qu'elle ne soit pas décelée par le Système de détection d'intrusions.

2.1.5.6 Sonde

C'est l'élément de l'architecture IDS qui collecte les informations brutes et en fournit une description à l'aide d'événements. C'est un ou plusieurs capteurs couplés avec un analyseur.

2.1.6 Les types de système de détection d'intrusions

Les données utilisées par les systèmes de détection d'intrusions peuvent provenir de sources variées. Elles peuvent être recueillies sur une machine ou sur tout un réseau. Il existe donc différents types d'IDS que nous allons décrire dans cette section.

2.1.6.1 Les systèmes de détection d'intrusions de type hôte (HIDS)

Un système de détection d'intrusions de type hôte (HIDS pour Host-based Intrusion Detection System) est caractérisé par l'analyse des événements et traces générés par le système d'une machine. Son objectif est de surveiller l'activité d'une machine unique donnée. A travers sa sonde logée sur un hôte singulier, il collecte des données produites par les systèmes d'exploitation des machines, notamment par le biais des journaux d'audit système ou par celui des appels système invoqués par les applications. Il s'insère entre les applications et le cœur du système d'exploitation pour protéger des applications ou des serveurs critiques. Son utilisation dans un réseau nécessite son installation sur chacun des systèmes à sécuriser. Dans des environnements plus larges, son déploiement est prohibitif en termes de coût et de maintenance. Son principal avantage est sa vue beaucoup plus profonde sur l'activité du système et se révèle plus précis dans sa stratégie de détection.

Dans cette catégorie, peuvent être distingués les IDS de niveau application, les programmes de vérification d'intégrité de fichiers et les IDS de niveau système. Les premiers examinent les opérations apparues dans une application pour détecter si elle est manipulée ou non ou si elle n'effectue pas des accès interdits vers des données sensibles. Une fois qu'un pirate prend le contrôle d'une machine par une application, il va essayer d'injecter du code malicieux. Cela pourrait affecter le système de fichiers. Il modifie le comportement de certains fichiers critiques tels que les dll (dynamically linked libraries), des programmes afin de créer une porte dérobée ou de rester indétectable tout en perpétrant son attaque. Ainsi certains programmes tels que Tripwire 3 sont utilisés pour vérifier l'intégrité des fichiers importants. Enfin certains IDS sont beaucoup rattachés au noyau système.

Un HIDS a une vue totalement limitée à un hôte, donc incapable de détecter les attaques ciblant plusieurs machines. Alors les IDS réseau font leur apparition.

2.1.6.2 Les systèmes de détection d'intrusions de type réseau (NIDS)

Un système de détection d'intrusions de type réseau (NIDS pour Network Intrusion Detection System) utilise les données réseau. Il analyse les paquets transitant sur un réseau afin d'identifier des anomalies. Son objectif est d'inspecter le trafic d'un grand nombre d'hôtes. Il écoute donc tout le trafic réseau. Trois technologies peuvent être distinguées à savoir :

- **Promiscous-mode NIDS :** ils fonctionnent en mettant une interface en mode promiscuous c'est-à-dire en écoute sur le réseau. Cela leur permet de pouvoir accéder à tout échange dans le réseau surveillé.
- **Network Node IDS :** ils s'intéressent seulement à des hôtes donnés. En effet les réseaux commutés empêchent les IDS précédents (Promiscousmode NIDS) de bien fonctionner car les paquets ne sont plus diffusés. Aussi la montée en débit des réseaux actuels entraîne la perte de paquets qui à priori est indésirable. Alors les Network Node IDS résolvent ces problèmes en spécialisant leurs analyses sur des hôtes particuliers.
- **Wireless Intrusion Detection Systems :** ce sont les types d'IDS destinés aux Réseaux Wifi. Ils sont réalisés pour surveiller les réseaux utilisant ce protocole qui n'est pas conçu à priori avec un esprit de sécurité.

Contrairement à un HIDS qui est restreint à un hôte, le NIDS à une vue plus générale sur l'ensemble du réseau ou du sous-réseau. Il permet donc de surveiller à moins de ressources tout un ensemble d'hôtes. Cette caractéristique simplifie le déploiement et la maintenance d'une

solution de détection visant à garantir une couverture optimale du réseau surveillé. L'approche système est plus complexe à déployer car elle nécessite une multiplication du nombre de capteurs dans le réseau. De plus, le coût engendré par la collecte des données par ces capteurs peut dégrader sensiblement les performances des systèmes sur lesquels ils sont installés.

Cependant, on peut s'interroger sur la pérennité des capteurs réseaux pour trois raisons principales. Premièrement, la montée en débit des réseaux contraint fortement les capacités de collecte de l'intégralité du trafic. Les constructeurs de NIDS ont recours à des capteurs matériels spécifiques pour accélérer la collecte, mais la détection d'intrusions dans le cœur de réseau peut poser problème car seules certaines données peuvent être prises en compte. L'inspection de la totalité des paquets n'étant pas envisageable, les IDS pour les réseaux à haut débit doivent échantillonner les données et l'analyse ne porte souvent que sur l'entête et la détection reste imprécise. Deuxièmement, les capteurs réseau ne peuvent analyser le trafic chiffré. Or, la prise en compte progressive des problèmes de sécurité tend à généraliser l'utilisation du chiffrement dans les protocoles réseau, rendant à terme les capteurs réseau inopérants. Enfin, l'analyse seule du trafic réseau s'avère souvent insuffisante pour assurer une détection fiable et pertinente des violations de politique de sécurité, l'IDS ne disposant que de trop peu d'informations sur les systèmes attaqués. Par ailleurs les NIDS sont en général victimes d'évasion et des attaques par déni de service.

2.1.6.3 Les solutions hybrides

Les IDS de type hybride intègrent les deux technologies précédentes dans leur fonctionnement pour bénéficier simultanément des avantages de l'une et de l'autre. Leur objectif est d'analyser les paquets réseaux mais aussi de suivre ce qui se passe exactement au niveau d'une machine de façon individuelle.

2.1.6.4 Les IPS

Contrairement à l'analyse passive réalisée par un IDS, un système de prévention d'intrusions (IPS pour Intrusion Prevention System) analyse de façon active les paquets. C'est un ensemble de composants logiciels et matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système. En gros, il fonctionne de manière similaire à un IDS mais non seulement il détecte l'intrusion mais aussi il prend des mesures actives contre celle-ci.

Plusieurs stratégies de prévention d'intrusions existent :

- Protection de mémoire et de processus (host-based memory and process protection) : surveille l'exécution des processus et les tue s'ils ont l'air dangereux (buffer overflow). Cette technologie est utilisée dans les KIPS (Kernel Intrusion Prevention System).
- Interception de session (session interception / session sniping) : termine une session TCP avec la commande TCP Reset : « RST ». Ceci est utilisé dans les NIPS.
- Routeur détecteur d'intrusions (gateway intrusion detection) : si un système NIPS est placé en tant que routeur, il bloque le trafic ; sinon il envoie des messages à d'autres routeurs pour modifier leur liste d'accès.

Un IPS possède de nombreux inconvénients. En effet, il bloque toute activité qui lui semble suspecte. Or, il est quasiment impossible d'assurer une fiabilité complète dans l'identification des attaques. Un IPS peut donc malencontreusement bloquer du trafic inoffensif. Par exemple, un IPS peut détecter une tentative de déni de service alors qu'il s'agit d'une période chargée en trafic. Les faux positifs sont donc très dangereux pour les IPS. Un autre inconvénient est qu'un pirate peut utiliser sa fonctionnalité de blocage pour mettre hors service un système. L'exemple d'un individu mal intentionné qui attaque un système protégé par un IPS, tout en spoofant son adresse IP en est un cas. Si l'adresse IP spoofée est celle d'un nœud important du réseau, les conséquences seront catastrophiques. Pour pallier ce problème, de nombreux IPS disposent des « white lists », c'est-à-dire des listes d'adresses réseaux qu'il ne faut en aucun cas bloquer. Autre inconvénient et non le moindre est qu'un IPS est peu discret. En effet, à chaque blocage d'attaque, il montre sa présence. Cela peut paraître anodin, mais si un pirate remarque la présence d'un IPS, il tentera de trouver une faille dans celui-ci afin de réintégrer son attaque mais cette fois en passant inaperçu. Voilà pourquoi les IDS passifs sont souvent préférés aux IPS. Cependant, il est intéressant de noter que plusieurs IDS (Ex : Bro, SNORT, RealSecure, Dragon, ...) ont été dotés d'une fonctionnalité de réaction automatique à certains types d'attaques.

2.1.6.5 Les IDS noyaux (KIDS/KIPS)

Dans le cadre du HIDS, l'utilisation d'un détecteur d'intrusions au niveau noyau peut s'avérer parfois nécessaire pour sécuriser une station. Il serait dangereux qu'un accès en lecture/écriture dans d'autres répertoires que celui consultable via http sur un serveur web, soit autorisé. Cela pourrait nuire à l'intégrité du système. Grâce à un KIPS, tout accès suspect peut être bloqué directement par le noyau, empêchant ainsi toute modification dangereuse pour le

système. Le KIDS est donc fortement lié au noyau du système et permet d'avoir un système en état sain. Le KIPS peut reconnaître des motifs caractéristiques du débordement de mémoire, et peut ainsi interdire l'exécution du code. Le KIPS peut également interdire l'OS d'exécuter un appel système qui ouvrirait un shell de commandes. Puisqu'un KIPS analyse les appels systèmes, il ralentit l'exécution. C'est pourquoi ce sont des solutions rarement utilisées sur des serveurs souvent sollicités. Un exemple de KIPS est SecureIIS, qui est une sur-couche du serveur IIS de Microsoft.

2.1.7 Les techniques de détection

Deux techniques principales sont utilisées en détection d'attaques : la première consiste à détecter une activité suspecte dans le comportement de l'utilisateur. La seconde, consiste quant à elle, à détecter des signatures d'attaques connues dans les paquets circulant sur le réseau. Ces deux techniques, aussi différentes soient-elles, peuvent être combinées au sein d'un même système afin d'accroître les possibilités de détection.

2.1.7.1 La détection par anomalie

Cette technique consiste à détecter une violation selon le comportement habituel de l'utilisateur. Pour cela, il faut préalablement dresser un profil utilisateur à partir de ses habitudes et déclencher une alerte lorsque des événements hors profil se produisent. Cette technique peut être appliquée non seulement à des utilisateurs mais aussi à des applications et services. Plusieurs métriques sont possibles : la charge CPU, le volume de données échangées, le temps de connexion aux serveurs, les protocoles et applications utilisés de façon habituelle, les heures de connexion, etc.

L'intérêt fort de l'analyse comportementale est qu'elle permet de détecter des attaques inconnues, contrairement à la seconde technique qui nécessite une connaissance préalable de l'attaque. Cependant elle souffre de beaucoup d'insuffisances. En effet, elle est peu fiable car tout changement dans les habitudes de l'utilisateur provoque une alerte. Aussi, elle nécessite une période de mise en œuvre des mécanismes d'auto-apprentissage. Si un pirate attaque pendant ce moment, ses actions seront assimilées à un profil utilisateur, et donc passeront inaperçues lorsque le système de détection sera complètement mis en place. L'établissement du profil doit être souple afin qu'il n'y ait pas trop de fausses alertes : le pirate peut discrètement intervenir pour modifier le profil de l'utilisateur afin d'obtenir après plusieurs jours ou semaines, un profil qui lui permettra de mettre en place son attaque sans qu'elle ne soit détectée.

Différentes méthodes ont été envisagées pour cette technique.

Approche probabiliste : des probabilités sont établies permettant de présenter une utilisation courante d'une application ou d'un protocole. Toute activité ne respectant pas le modèle probabiliste provoquera la génération d'une alerte.

Approche statistique : le but est de quantifier les paramètres liés à l'utilisateur : taux d'occupation de la mémoire, utilisation des processeurs, valeur de la charge réseau, nombre d'accès à l'intranet par jour, vitesse de frappe au clavier, sites les plus visités, etc. Elle est actuellement plus explorée dans les recherches, où les chercheurs utilisent des réseaux neuronaux et la fouille de données pour tenter d'avoir des résultats convaincants.

2.1.7.2 La détection par signature

Également appelée détection par scénario, cette technique s'appuie sur la connaissance des techniques utilisées par les attaquants pour déduire des scénarios typiques. Elle ne tient pas compte des actions passées de l'utilisateur et utilise des signatures d'attaques, ensemble de caractéristiques permettant d'identifier une activité intrusive : une chaîne alphanumérique, une taille de paquet inhabituelle, une trame formatée de manière suspecte. Elle se base sur la recherche de motifs (chaînes de caractères ou suite d'octets) au sein du flux de données. L'IDS comporte une base de signatures où chaque signature contient les protocole et port utilisés par l'attaque ainsi que le motif qui permettra de reconnaître les paquets suspects.

Comme principal inconvénient, seules les attaques possédant une signature sont détectées. En effet, à l'instar des antivirus, cette méthode utilise une base de signatures. Il est donc nécessaire de mettre à jour régulièrement la base. Par ailleurs, les motifs sont en général fixes. Or, une attaque peut être changée dans le temps par le pirate. Le moindre octet différent par rapport à la signature provoquera la non détection de l'attaque.

En général, l'analyse de conformité des paquets aux RFC, à l'aide de préprocesseurs, où chaque préprocesseur est chargé d'analyser un protocole particulier (FTP, HTTP, ICMP, etc), se rapporte à la détection par scénario.

2.1.8 Déploiement des IDS

Plusieurs architectures sont possibles pour le déploiement d'un IDS. En général, les configurations possibles sont : l'architecture avec un seul capteur, l'architecture distribuée et l'architecture centralisée.

Il est important de rappeler qu'il y a les IDS de type hôte (HIDS) et les IDS de type réseau (NIDS). Les HIDS par définition analysent les données (les appels systèmes, les journaux d'événements) sur une machine donnée. Ils fonctionnement donc sur un hôte particulier et sont autonomes. Par contre les NIDS s'occupent d'un segment de réseau. Ils sont donc déployés de façon à surveiller un ensemble de machines. Cela nécessite de leur donner une position précise afin de tirer profit de cette capacité.

Cela offre l'avantage au NIDS de n'analyser que les données validées par le pare-feu. Le taux d'alerte pourrait ainsi en être réduit. Cependant d'autres administrateurs préfèrent le placer avant le pare-feu dans le souci d'être informés de tout ou de tout constater.

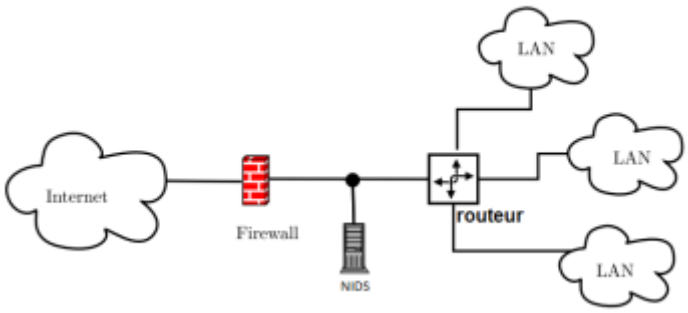


Figure 21 : Déploiement typique d'un NIDS

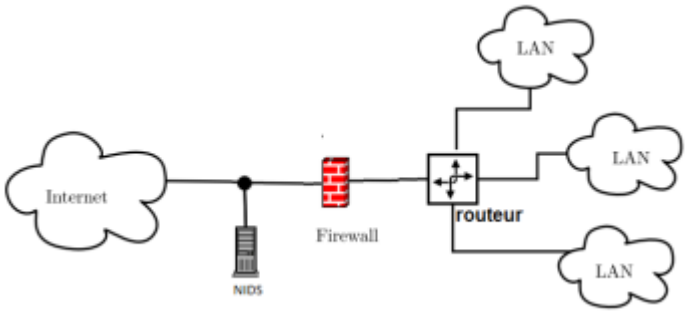


Figure 22: Autre déploiement de NIDS

Nous venons de présenter les systèmes de détection et de prévention d'intrusion ainsi que la place qu'ils occupent aujourd'hui dans l'arsenal de sécurité des organisations. Nous allons maintenant passer au prochain point consacré nous à l'étude des pots de miel.

2.2 Les pots de miel

Un pot de miel est un outil fréquemment utilisé dans le domaine de la sécurité informatique. Il est installé pour être compromis, dans le but de recueillir des informations sur les actions des pirates. Ce chapitre contient une présentation globale des pots de miel et détaille leur fonctionnement et déploiement dans un réseau informatique.

2.2.1 Définition

Dans la littérature, la définition proposée pour les pots de miel varie d'un auteur à un autre selon le contexte d'utilisation. En effet, certains considèrent qu'un pot de miel est un outil pour attirer les attaquants alors que d'autres le considèrent plutôt comme un outil de détection d'intrusions. Pour Yegneswaran et Al. , les pots de miel sont des systèmes déployés sur internet pour le seul but d'être compromis afin de permettre l'étude du comportement des pirates. Lance Spitzner propose qu'il s'agît d'une ressource de sécurité déployée et dont l'objectif est d'être sondée, attaquée ou compromise. C'est aussi une machine placée dans un réseau mais dont personne ne se sert. En théorie, aucune connexion de ou vers cette machine ne devrait être observée [13].

En somme, on peut noter qu'un pot de miel est un système destiné à piéger les pirates pour apprendre les outils, les stratégies et les comportements qu'ils adoptent quand ils veulent s'introduire dans un réseau ou un système.

2.2.2Historique

Le concept des pots de miel a publiquement fait son apparition en 1990 avec les œuvres « The Cuckoo's Egg» et «An Evening With Berferd» respectivement de Clifford Stoll et de Bill Cheswick qui décrivaient l'idée de suivre un pirate dans son activité. En effet, ces œuvres s'inspiraient de l'observation du fonctionnement d'un intrus qui a pu s'introduire dans un ordinateur du laboratoire LBNL 1. Cette observation a permis de tracer le processus d'attaque du pirate. En 1997, le premier pot de miel Deception ToolKits (DTK) fut publié par Fred Cohen. CyberCop Sting fut commercialisé en 1998 avec le concept de plusieurs systèmes virtuels. Cette même année BackOfficer Friendly fut publié, gratuit et simple d'utilisation, ne s'installant que

sur la plateforme Windows. En 1999, Honeynet Project prit naissance avec l'idée de former un réseau de pots de miel. Plus tard, plusieurs projets similaires tels que Leurré.com et WOMBAT ont été définis dans différent pays, pour décentraliser la collecte d'informations sur les attaques système. En 2000, alors les pots de miel commencèrent à être utilisés pour capturer et étudier les activités des vers (worms). Par ailleurs, plusieurs organisations commencèrent à les déployer pour l'étude des nouvelles attaques basées sur les vulnérabilités non encore révélées.

2.2.3 Principe de fonctionnement

Comme souligné précédemment, les pots de miel (Honeypots) sont des systèmes informatiques configurés dans le but qu'ils soient compromis, sondés ou attaqués par les pirates informatiques. En sécurité informatique ils constituent une source d'information remarquable sur la nature des attaquants, leurs objectifs, leurs méthodes d'attaques et leurs comportements face aux différents systèmes. L'idée est de mettre en place un moyen pour contrôler les attaques et les activités des attaquants en leur donnant accès à quelques services, parfois émulés, tout en limitant les dégâts possibles de ces attaques puisque l'attaquant n'a pas accès aux serveurs réels en production.

Cependant, la richesse de l'information recueillie est directement proportionnelle au degré d'interaction offert par le pot de miel. Ainsi, si les services offerts sont très limités, le pot de miel sera moins attractif donc moins intéressant pour le pirate qui maintient alors moins de dialogue et peut même détecter l'existence de cette duperie.

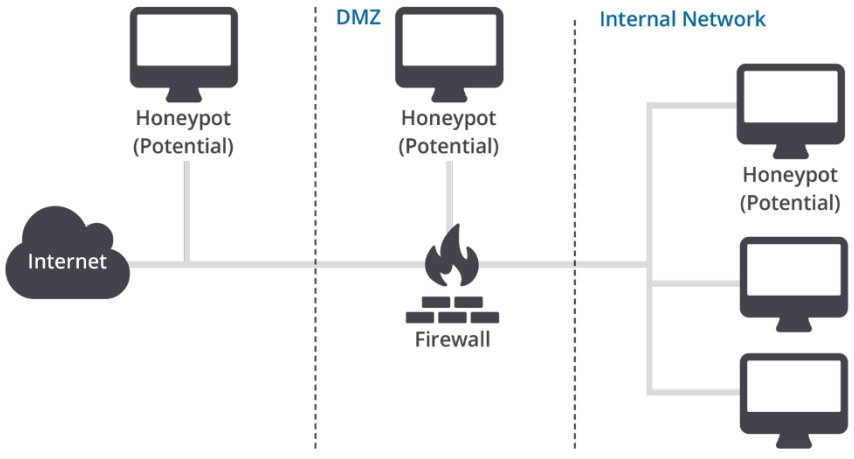


Figure 23: Déploiement pot de miel [13]

2.2.4 Avantages et inconvénients des pots de miel

Les pots de miel informatiques permettent de détecter les attaques, de les détourner de cibles plus intéressantes et de recueillir des informations sur les cybercriminels et leurs tactiques. Ils peuvent révéler :

- **Localiser l'adresse IP du cybercriminel.** Ces données peuvent révéler leur emplacement ou leur identité, sauf si le pirate utilise un VPN ou un serveur proxy ;
- **Le type de mots de passe que les pirates ont utilisé pour y accéder**. Peut-être ont-ils utilisé des mots de passe qui ont fuité. Il est donc temps d'utiliser des mots de passe sécurisés, complexes et uniques. Pour vous faciliter la tâche, NordPass peut vous aider à stocker vos mots de passe en toute sécurité ;
- **La technique utilisée pour pénétrer dans le honeypot**, qui peut révéler les vulnérabilités de votre système et de vos serveurs web ;
- **Où sont allés vos fichiers volés.** Les pots de miel peuvent stocker des données avec des identifiants uniques, qui (lorsqu'ils sont volés) peuvent aider leurs propriétaires à trouver où les données ont été envoyées. Ils peuvent également aider à identifier les liens entre différents pirates.

Les honeypots sont donc d'excellents outils de ruse, largement utilisés par les grandes entreprises et les chercheurs en sécurité. Il existe de nombreuses configurations de pots de miel qui sont pour la plupart gratuites et en open source. Certaines peuvent simuler des serveurs et vous aider à analyser les données, vous évitant ainsi d'avoir recours à une grande équipe de recherche.

Autres avantages du honeypot :

- Même si les cybercriminels chiffrent leurs données, les honeypots peuvent détecter toute activité suspecte.
- Comme les utilisateurs réguliers n'ont pas besoin d'accéder aux honeypots, ces derniers permettent de réduire considérablement le nombre de fausses alertes.
- Ils permettent de récolter et d'analyser un large volume de données, toutes relatives à des activités malveillantes.
- Ils représentent une source d'informations importante pour les analystes et chercheurs sur les attaques réelles et des activités malveillantes.

- Cet outil peut aussi vous permettre de lutter contre les ransomwares. En effet, en créant un honeypot avec des faux fichiers, vous pouvez surveiller les interactions et ainsi repérer plus facilement les activités suspectes.

Aussi performants soient-ils, les honeypots présentent certaines limites et vulnérabilités.

- Ils ne collectent des données que lorsqu'il y a une attaque.
- Ils ne sont pas vraiment confidentiels. Les pirates expérimentés peuvent utiliser des techniques d'empreinte digitale pour identifier un pot de miel. Par conséquent, ils l'éviteront et pourront éventuellement porter leur attention sur un réseau ou un serveur plus intéressant.
- Ils ne peuvent pas détecter les attaques extérieures à leurs systèmes.
- S'ils ne sont pas configurés correctement, en particulier un pot de miel pur, ils peuvent agir comme une passerelle vers d'autres systèmes et réseaux.
- Comme tout autre système d'exploitation, ils peuvent présenter des vulnérabilités technologiques telles que des pares-feux et des chiffrements faibles ou peuvent tout simplement ne pas identifier les attaques. Les pots de miel ne sont tout simplement pas parfaits.

2.2.5 Classification des pots de miel

Les systèmes de honeypots peuvent être classés comme suit :

Les honeypots purs, qui sont des systèmes de production complets ne nécessitant aucun autre logiciel. En d'autres termes, ce sont des serveurs de production transformés en pots de miel, et ils sont connectés au reste du réseau. Ce sont les plus crédibles, mais aussi les plus risqués et les plus coûteux.

Les pots de miel à forte interaction sont des systèmes d'exploitation non émulés. Ils imitent les systèmes de production et comportent généralement beaucoup de services et de données. Ils nécessitent donc beaucoup de ressources pour fonctionner. Ces honeypots sont en temps normal exécutés sur des machines virtuelles (VM), ce qui permet à plusieurs d'entre eux de fonctionner sur un seul appareil. Cela facilite également le sandboxing (isolation) des systèmes compromis, leur arrêt et leur restauration.

Les pots de miel à faible interaction n'émulent que le système ou le service le plus recherché. Ils nécessitent moins de ressources et sont également utilisés principalement sur des machines virtuelles. Ils sont donc moins risqués et plus faciles à maintenir. D'un autre côté, ils sont plus faciles à identifier par les pirates et sont mieux utilisés pour détecter les logiciels malveillants diffusés par les réseaux de botnets et les vers.

2.2.6 Déploiement d'un pot de miel

Il existe deux catégories de pots de miel selon le contexte d'utilisation : les pots de miel de production et les pots de miel de recherche.

Les pots de miel de production sont utilisés pour renforcer l'arsenal de sécurité d'une organisation. Ils sont utilisés notamment pour détecter les intrusions, les activités non autorisées et offrent de la flexibilité dans l'analyse des attaques. Ils sont installés dans la DMZ en simulant les services offerts par l'organisation. Cela permet d'étudier les attaques éventuelles contre les serveurs du réseau.

Un des problèmes en sécurité est le manque d'informations utiles sur les pirates. Alors les pots de miel de recherche sont utilisés pour étudier qui sont les attaquants, pourquoi est-ce qu'ils attaquent, comment ils attaquent, les outils qu'ils utilisent et comment ils procèdent une fois qu'ils prennent le contrôle d'une machine. Les pots de miel de recherche visent à rassembler le maximum d'informations sur les pirates afin d'offrir le moyen de mieux se défendre contre eux. Le déploiement de ces pots de miel dépend des objectifs visés par les chercheurs. Ils sont parfois mondialement déployés, formant un réseau comme dans les projets

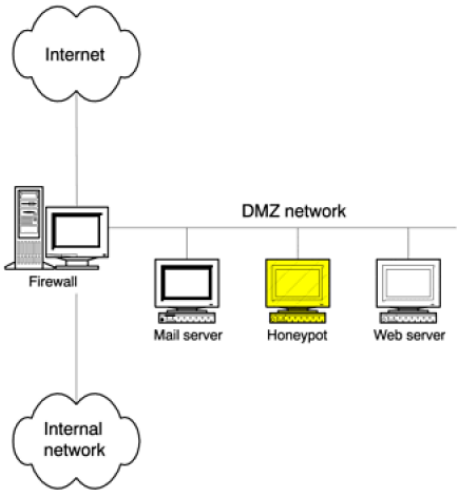


Figure 24 : Déploiement classique d'un pot de miel de production

2.2.7 Honeynets

Un honeynet est un réseau de pots de miel. Il est utilisé dans un but de recherche et comporte de véritables machines tournant différents systèmes et applications, de quoi offrir aux pirates un environnement identique aux environnements de production. Ses objectifs sont de mieux connaitre qui sont les pirates, les outils et les tactiques qu'ils emploient, leurs motivations ; de profondes informations qu'aucun autre type de pot de miel n'est en mesure de fournir. Le honeynet permet, ainsi, de surveiller et d'enregistrer ensuite toutes les actions malicieuses des attaquants. Par ailleurs, sa structure en réseau offre l'avantage d'avoir des renseignements sur les communications entre les attaquants et leurs méthodes de collaboration. Ainsi, le honeynet est considéré comme un outil de premier choix pour apprendre les techniques d'attaques, et les comportements des attaquants, sur un réseau réel. Complexe et difficile à configurer, il utilise une variété de systèmes pour détecter plusieurs types d'attaques : ceux qui sont connus et ceux qui ne le sont pas (zero day). Sa conception nécessite trois contraintes majeures à prendre en compte à savoir le contrôle de données, la capture de données et la collecte de données.

Le contrôle de données est l'ensemble des techniques à mettre en œuvre pour contrôler l'activité du pirate une fois qu'il a pris le contrôle d'une machine du honeynet, afin de limiter les risques liés à ses actions. La capture de données constitue les moyens à déployer pour enregistrer de façon sécurisée les activités du pirate. La collecte de données apparait lorsqu'il s'agit de récupérer des données de plusieurs honeynets. Il faut alors disposer des outils nécessaires pour la collecte et le traitement de ces données de différentes origines.

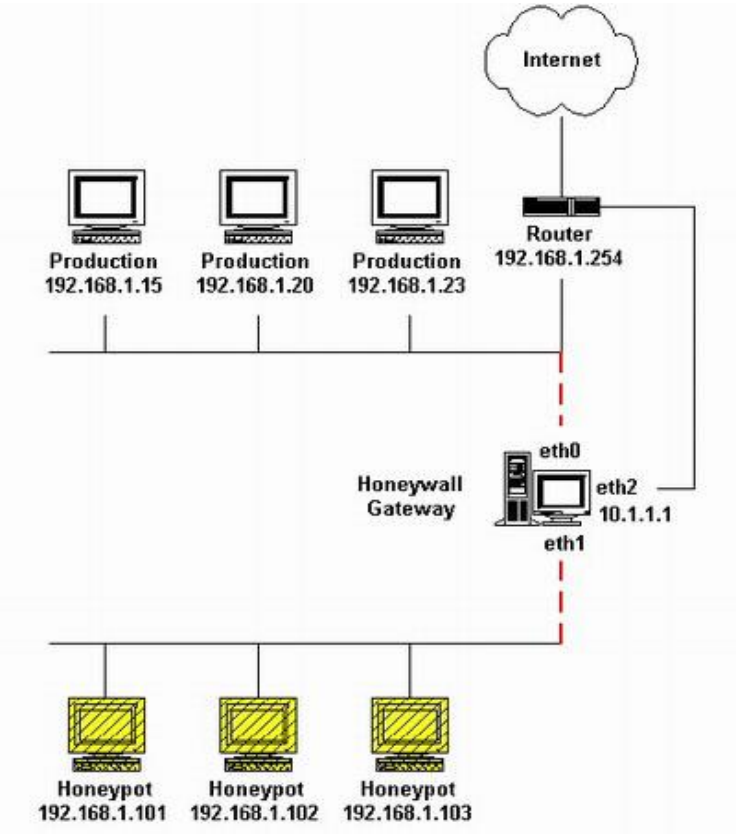


Figure 25: Représentation d'un honeynet [10]

Nous venons de passer en revue la technologie des pots de miel. Très utiles en termes de fonctionnalité, ils sont utilisés pour compléter le paquetage sécuritaire d'une organisation ou pour des fins de recherche. Du fait de l'agrandissement des réseaux d'entreprises, l'augmentation des débits ainsi que la prolifération des attaques, une simple sonde de détection s'est très vite révélée insuffisante. Les développeurs d'outils de sécurité ont alors très tôt pensé aux architectures impliquant plus de capteurs. Cela constitue l'objet de notre prochain point qui en fait une étude détaillée.

2.3 La détection distribuée d'intrusions

Les systèmes de détection d'intrusions (IDS) souffrent généralement de certaines insuffisances. Le principal défaut des premières architectures est qu'elles sont bâties autour d'une seule entité monolithique qui effectue la plus grande partie des calculs et de la collecte d'informations. Par ailleurs, l'augmentation de l'activité malveillante sur Internet et la montée des débits au niveau du réseau, ont précipité le besoin d'IDS de grandes possibilités. On parle de systèmes distribués.

Ces systèmes de détection d'intrusions distribués multiplient la capacité d'un simple IDS en utilisant un ensemble d'événements obtenu d'un environnement géographiquement dispersé.

2.3.1 Définition

Un système de détection distribué (dIDS : distributed Intrusion Detection System) constitue un ensemble de systèmes dans un environnement large, chacun communicant avec les autres, ou avec un serveur central qui facilite la surveillance plus efficace d'un grand réseau, l'analyse d'incidents. A l'aide de ces agents coopératifs distribués à travers un réseau, les experts de la sécurité et les administrateurs de réseau ont une vue assez globale sur les événements apparus dans tout un réseau, aussi large soit-il.

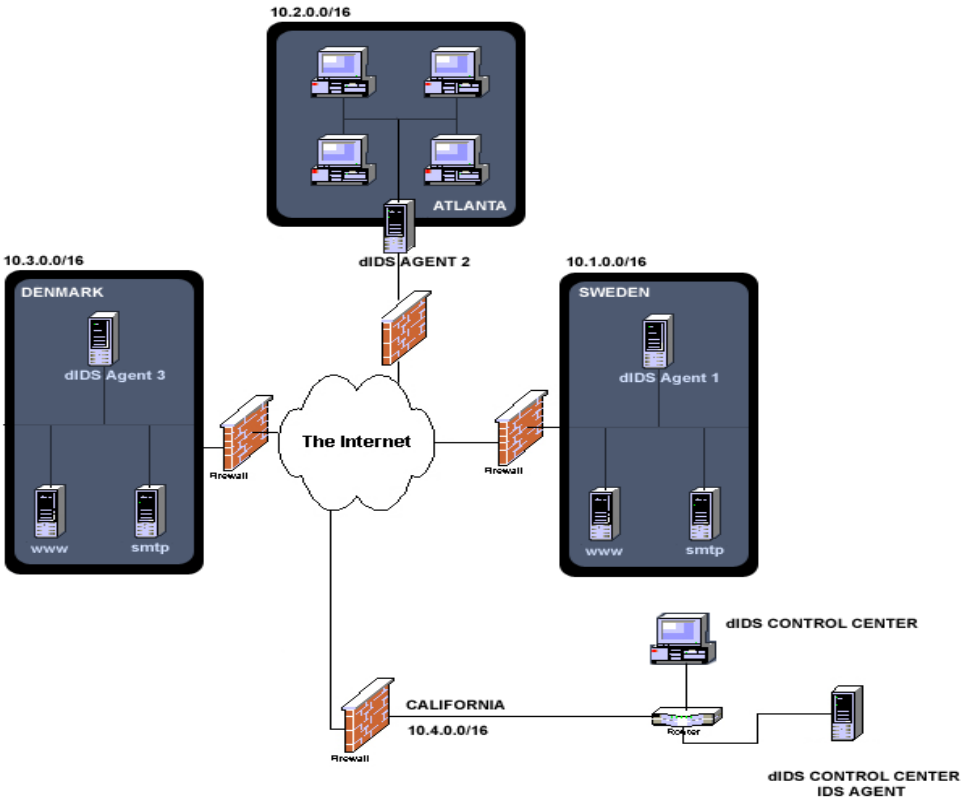


Figure 26: Fonctionnement d'un DIDS [11]

2.3.2 Avantages

L'apparition des dIDS est essentiellement approuvée par les limites d'un simple IDS, à savoir :

- ✓ L'existence d'attaque ne pouvant pas être détectée par l'observation d'un seul site (ex : botnet) ;
- ✓ Les attaques coordonnées impliquent plusieurs pirates nécessitant une vue globale d'analyse ;
- ✓ Le changement dans la conduite de l'attaque qui cause la fausse détection ou identification ;
- ✓ La détection d'intention d'attaque et des tendances d'attaque qui sont nécessaires pour prévenir ;
- ✓ L'apparition des attaques autonomes et automatisées, des vers avancés qui nécessitent une analyse rapide et avancée ;

- ✓ La concrétisation de plusieurs attaques due au manque de partage d'information entre organisations qui refusent de se partager les données de sécurité.

Le principe de la détection distribuée consiste donc à disposer plusieurs sondes dans différents sites d'un réseau. Il s'agit de multiplier la source de capture de données ou le traitement de ces données. Donc une architecture distribuée se base sur l'une de ces options ou les deux à la fois. Cela permet :

- De disposer d'informations bien hétérogènes afin de ne pas faire des conclusions qui ne se rapportent qu'à une région donnée ou une partie de réseau ;
- De pouvoir supporter la charge réseau ;
- De mettre en place des mécanismes de collaboration afin de réduire autant que possible les effets d'une intrusion, surtout une attaque non découverte ou basée sur des vulnérabilités non encore connues (zero-dayattacks) ;
- L'analyse d'incidents plus précise et plus flexible. C'est une des raisons fondamentales pour lesquelles les dIDS ont été conçus. C'est une analyse plus avancée des attaques apparues sur plusieurs segments d'un réseau.

2.3.3 Les différentes technologies distribuées

La détection distribuée peut être réalisée suivant trois schémas différents : Le load-balancing, les agents non autonomes distribués et le partage d'informations entre instances autonomes.

2.3.3.1 Le load-balancing

Le load-balancing consiste en la répartition de la charge réseau entre plusieurs instances. Cette répartition peut être statique, basée sur les adresses IP ou les protocoles d'application (HTTP, FTP, ICMP) ou dynamique. C'est une technologie adéquate aux réseaux à haut débit dont le flux de paquets ne peut être analysé par une seule instance d'IDS. Elle apporte donc une solution à la gestion de la quantité de paquets qui constitue un défi pour les IDS. Cependant, d'autres problématiques surgissent. En effet, le scan de réseau et les attaques visant plusieurs machines à la fois ne sont plus détectables sans mécanismes spécifiques de corrélation d'alertes.

2.3.3.2 Les agents non autonomes distribués

La deuxième architecture est basée sur la distribution de capteurs à différents endroits sur le réseau. Ces capteurs réalisent généralement des analyses de bas niveau comme le décodage de protocoles ou la détection de signatures. Ils envoient ensuite leurs données vers un analyseur qui corrèle le tout. Dans cette architecture, tous les éléments collaborent pour effectuer la tâche. Aucun agent n'est autonome. Malgré son avantage de disposer d'informations de différents endroits, cette architecture a de grands défauts. En effet le serveur central constitue un goulot d'étranglement et nécessite généralement de machines spécifiques car il effectue pratiquement seul tout le traitement interne, donc a besoin de beaucoup de ressources.

2.3.3.3 Les agents autonomes

La troisième approche vise le partage d'informations entre instances totalement autonomes. Ainsi on peut par exemple partager des données liées à l'activité d'un pirate afin de limiter ses effets possibles sur le réseau. On peut également se partager des sources d'adresse que l'on décide de bloquer.

2.3.4 La corrélation d'alertes

La corrélation d'alertes est la technique permettant de générer une alerte à partir de plusieurs alertes provenues d'une ou de plusieurs sources. Les alertes généralement produites par les IDS sont nombreuses, manquent de précision et sont souvent parcellaires. Ces alertes sont par conséquent d'un intérêt limité pour un opérateur humain. La corrélation d'alertes est donc d'un intérêt très prometteur. Trois objectifs principaux motivent cette technique à savoir :

- La réduction du volume d'informations à traiter par les opérateurs et les analystes notamment à l'aide des techniques d'agrégation ;
- L'augmentation de la qualité du diagnostic fourni ;
- Le suivi des attaques au cours du temps.

Les travaux autour de cette technique dans le domaine de la détection d'intrusions sont relativement récents. Dans la littérature, on peut toutefois identifier deux approches principales de corrélation.

Corrélation implicite : l'exploitation des alertes révèle des relations intrinsèques entre elles. Une relation peut être constituée par exemple par une correspondance fréquentielle ou statistique entre des alertes. Cette correspondance est obtenue par une analyse automatique des données.

Corrélation explicite : l'opérateur est capable d'exprimer explicitement des relations entre différentes alertes, sous la forme d'un scénario. Un scénario regroupe en général un ensemble de propriétés que doivent satisfaire les alertes, et des liens les connectant.

2.3.5 Quelques travaux

Le domaine de la détection distribuée a été largement défriché. Ainsi plusieurs travaux ont été menés. DIDS (Distributed Intrusion Detection System) ouvre la voie à la détection distribuée par l'utilisation de sondes de type hôte et réseau. Ces différentes sondes envoient les données collectées à un serveur central qui réalise l'analyse sémantique de ces événements.

CSM (Cooperating Security Managers) utilise une architecture décentralisée composée d'un ensemble d'IDS locaux présents sur chaque machine. Par ailleurs, chaque IDS est doté d'une fonction spécifique de coordination avec les autres en vue de détecter les attaques distribuées.

AAFID (Autonomous Agents for Intrusion Detection) propose une architecture basée sur des agents autonomes organisés en plusieurs couches hiérarchiquement organisées avec chaque couche réalisant une fonction spéciale.

DIDMA (Distributed Intrusion Detection using Mobile Agents) se sert de deux types d'agents : les agents statiques et les agents mobiles. Chaque système à surveiller est pourvu d'un agent statique. Chaque fois qu'il y a une activité suspecte, ce dernier informe le MAD (Mobile Agents Dispatcher) qui génère un agent mobile envoyé vers toutes les machines qui ont émis des alertes. Cet agent mobile analyse toutes les machines concernées et génère une alerte si nécessaire.

Emerald (Event monitoring enabling responses to anomalou live disturbances) organise de façon hiérarchique les analyseurs qui échangent des résultats d'analyse et peuvent souscrire à des services les uns chez les autres. La structure hiérarchique permet de propager l'information jusqu'à une racine donnée.

GrIDS(Graph-based Intrusion Detection System) modélise les attaques par des graphes d'activité. Ses composants analysent le trafic à différents endroits puis se communiquent des informations.

Dans le tableau suivant, nous présentons quelques principaux IDS à architecture distribuée avec leurs caractéristiques.

Tableau 4 : Principaux IDS distribués et leurs caractéristiques

IDS	Source des données analysées	Approche	Prétraitement à distance	Détection centralisée	Analyse en temps réel	Type de réponse
AAFID	Système	Scénarios	Oui	Oui	Oui	Passive
DIDS	Système Réseau	Hybride	Oui	Oui	Oui	Passive
DPEM	Système	Comporte mentale	Oui	Oui	Oui	Passive
GrIDS	Système Réseau	Hybride	Oui	Oui	Non	Passive
CSM	Système	Comporte mentale	Oui	Non	Oui	Active
IDA	Système	Scénarios	Agents mobiles	Oui	Oui	Passive

2.4 Choix des outils

Nous nous intéressons plus aux NIDS c'est-à-dire des IDS de type réseau et il existe un grand nombre d'IDS de ce type dont SNORT, SURICATA, BRO(Zeek). Nous allons donner un bref aperçu et faire une comparaison de ces types d'NIDS.

2.4.1 Les systèmes de détection d'intrusion basés sur le réseau (NIDS)

Les systèmes de détection d'intrusion basés sur le réseau (NIDS) fonctionnent en inspectant tout le trafic sur un segment de réseau afin de détecter les activités malveillantes.

Avec les NIDS, une copie du trafic traversant le réseau est délivrée au dispositif NIDS en mettant en miroir le trafic traversant les commutateurs et/ou les routeurs.

Un dispositif NIDS surveille et alerte sur des modèles de trafic ou des signatures. Lorsque des événements malveillants sont signalés par le dispositif NIDS, des informations vitales sont enregistrées. Ces données doivent être surveillées afin de savoir qu'un événement s'est produit. En combinant ces informations avec les événements collectés par d'autres systèmes et dispositifs, vous pouvez obtenir une image complète de la posture de sécurité de votre réseau. A notez qu'aucun des outils présentés ici ne corrèle les journaux par lui-même. C'est généralement la fonction d'un gestionnaire d'informations et d'événements de sécurité (SIEM).

2.4.2 Snort

Snort est un système de détection d'intrusion et de prévention d'intrusion gratuit et open-source créé en 1998 par Martin Roesch. Développé à l'origine par la société Sourcefire, il est aujourd'hui maintenu par Cisco Systems à la suite du rachat de Sourcefire en 2013. Beaucoup de gens se souviendront de 1998 comme de l'année de sortie de Windows 98, mais c'est aussi l'année où Martin Roesch a publié pour la première fois Snort. Bien que Snort ne soit pas un véritable IDS très connu à l'époque, il est devenu de nos jours une référence pour les IDS, grâce aux contributions de la communauté.

Il est important de noter que Snort n'a pas de véritable interface graphique ou de console d'administration facile à utiliser, bien que beaucoup d'autres outils open source aient été créés pour aider, comme BASE et Sguil. Ces outils fournissent une interface web pour interroger et analyser les alertes provenant de Snort IDS.

Résumé de Snort

- Longue durée de vie du produit sans aucun signe de disparition
- Grande assistance communautaire
- Plusieurs frontaux administratifs
- Eprouvés et testés
- Grande assistance communautaire

Selon le site Web de Snort, les caractéristiques comprennent :

- ✓ Conception modulaire :
- ✓ Multi-threading pour le traitement des paquets ;
- ✓ Configuration partagée et table attributaire ;
- ✓ Utilisez une configuration simple de script ;
- ✓ Services de détection automatique pour la configuration sans port ;
- ✓ Génération automatique de la documentation de référence ;
- ✓ Profil de mémoire évolutif ;
- ✓ Analyseur de règles et syntaxe.

Documentation :

- ✓ Mises à jour des ensembles de règles ;
- ✓ Snort FAQ ;
- ✓ Une feuille de triche Snort ;
- ✓ Un plugin pour Snort est disponible.

2.4.3 Suricata

Suricata est un logiciel open source de détection d'intrusion, de prévention d'intrusion, et de supervision de sécurité réseau. Il est développé par la fondation OISF. Suricata permet l'inspection des Paquets en Profondeur.

Il existe des outils tiers open-source disponibles pour un frontal web permettant d'interroger et d'analyser les alertes provenant de Suricata IDS.

Résumé de Suricata

- Multi-Threaded – Snort fonctionne avec un seul thread, ce qui signifie qu'il ne peut utiliser qu'un CPU (core) à la fois. Suricata peut exécuter de nombreux threads afin qu'il puisse profiter de tous les cpu/cores dont vous disposez.
- Accélération matérielle intégrée ;
- Extraction de fichiers : Si quelqu'un télécharge un logiciel malveillant, Vous pouvez le capturer directement depuis Suricata et l'étudier.

- LuaJIT : C'est un moteur de script qui peut être utilisé avec les informations des paquets inspectés par Suricata. Cela rend les correspondances complexes encore plus faciles et vous pouvez même gagner en efficacité en combinant plusieurs règles en un seul script.
- La journalisation de plus que les paquets : Suricata peut saisir et enregistrer des choses comme les certs TLS/SSL, les requêtes HTTP, les requêtes DNS
- Grande assistance communautaire

Selon le site Web de Suricata, les caractéristiques comprennent :

- ✓ Hautes performances : base de code multithread et évolutive
- ✓ Moteur polyvalent : NIDS, NIPS, NSM, analyse hors ligne, etc.
- ✓ Prise en charge multiplateforme : Linux, Windows, macOS, OpenBSD, etc.
- ✓ Prise en charge moderne de TCP/IP, y compris un moteur de flux évolutif, IPv4/IPv6 complet, flux TCP et défragmentation des paquets IP
- ✓ Analyseurs de protocole – décodage de paquets, décodage de couche d'application
- ✓ Moteur HTTP – analyseur de flux HTTP, enregistreur de requêtes, correspondance de mots clés, etc.
- ✓ Services de détection automatique pour la configuration sans port
- ✓ Script Lua (LuaJIT)
- ✓ Journalisation et analyse de la couche applicative, y compris les certificats TLS/SSL, les requêtes HTTP, les requêtes DNS, etc.
- ✓ Accélération matérielle intégrée (GPU pour le reniflage réseau)
- ✓ Extraction de fichiers

Documentation :

- ✓ Suricata Guide de l'utilisateur
- ✓ Documents utilisateur et développeur
- ✓ Suricata FAQ

2.4.4 Bro (Zeek)

Bro, qui a été renommé Zeek à la fin de 2018 et est parfois appelé Bro-IDS ou maintenant Zeek-IDS, est un peu différent de Snort et Suricata. Bro est à la fois un IDS basé sur la signature et les anomalies. Son moteur d'analyse converti le trafic capturé en une série d'événements. Un événement peut être une connexion utilisateur à FTP, une connexion à un site Web ou pratiquement n'importe quoi. La puissance du système est ce qui vient après le moteur d'événements et c'est l'interpréteur de script de stratégie. Ce moteur de politiques à son propre langage (Bro-Script) et il peut effectuer des tâches très puissantes et polyvalentes.

Il n'y a pas d'interface graphique native, mais il existe des outils tiers open-source disponibles pour un front-end web pour interroger et analyser les alertes provenant de Bro-IDS.

Résumé de Bro

- Compliqué à mettre en place
- Peut détecter des modèles d'activité que d'autres systèmes IDS ne peuvent pas
- Architecture très extensible
- Bon soutien de la communauté

Selon le site Web de Bro, les fonctionnalités comprennent :

- ✓ Journalisation et analyse complètes du trafic
- ✓ Langage de script événementiel puissant et flexible (scripts Bro)
- ✓ Déploiement sur des systèmes de type UNIX, y compris Linux, FreeBSD et MacOS
- ✓ Prise en charge des protocoles DNS/FTP/HTTP/IRC/SMTP/SSH/SSL/autres protocoles
- ✓ Analyse entièrement passive du trafic avec robinet réseau ou port de surveillance
- ✓ Analyse en temps réel et hors ligne
- ✓ Prise en charge des clusters pour les déploiements à grande échelle
- ✓ Prise en charge complète d'IPv6
- ✓ Correspondance de modèle de style IDS
- ✓ Extraction de fichiers

- ✓ Architecture extensible
- ✓ Les analystes peuvent utiliser Bro pour l'automatisation (extraction de fichiers, analyse de logiciels malveillants, liste noire, suivi des modèles d'utilisation, travaux de recherche, etc.)

Documentation :

- ✓ Manuel de Bro
- ✓ Docs de Bro
- ✓ Foire aux questions de Bro

2.4.5 Comparaison des solutions

La comparaison des différents NIDS va nous permettre d'être fixé sur la meilleure technologie de NIDS à utiliser au long de notre projet. Le tableau suivant montre une brève comparaison des NIDS les plus connu et disponible nous permettant ainsi d'affiner notre choix en fonction de notre besoin.

Tableau 5: Comparaison des NIDS

NIDS	Bro (Zeek)	Suricata	SNORT
Valeur	Logiciel gratuit	Logiciel gratuit	Logiciel gratuit
Meilleure utilisation	NIDS open source	NIDS Multi-thread	Reniflage de paquets
Principales caractéristiques du produit	Enregistrement du trafic Analyse des menaces Personnalisation des scripts	Grande performance Détection de protocole Décodage de paquets	Surveillance des journaux Temps réel Détection basée sur des règles
Résumé	Il intègre un atout majeur : l'analyse de flux réseau. Cette analyse permet de concevoir une cartographie du réseau et d'en générer un modèle. Ce modèle est comparé en temps réel au flux de données et toute déviance lève une alerte	Concurrent raisonnable de Snort, avec un support multi-threading. Le manque de documentation rend la configuration et la maintenance difficiles	Bon outil open source gratuit, mais courbe d'apprentissage abrupte et difficile à configurer

Conclusion partielle

En résumé, la détection distribuée consiste en l'analyse de données recueillies à partir de plusieurs capteurs distribués dans un réseau. Nous avons exposé les différentes possibilités à savoir le load-balancing, les agents non autonomes distribués et les agents autonomes.

La prochaine partie de ce document est consacrée à l'analyse et la mise en œuvre de la solution de détection et prévention d'intrusion à partir des capteurs distribués dans un réseau informatique.

PARTIE 2 : Analyse et conception

Cette partie est subdivisé en 3 chapitres à savoir, matériel et méthodes, la rédaction d'un cahier de charge, l'implémentation et les résultats de notre solution.

Chapitre 3 : Matériel et méthode

Dans ce chapitre, nous présentons l'ensemble du matériel et des méthodes nécessaires à la réalisation de notre travail.

3 Matériel et méthode

L'analyse fonctionnelle d'un projet informatique est une étape qui s'avère nécessaire et primordial pour mener à bien ce dernier. Elle permet de concevoir un système pour lequel toutes les options seront parfaitement conçues, orientées vers une satisfaction client maximale. C'est dans cette optique qu'avant de commencer ce projet, nous analyserons de manière exhaustive son environnement afin de comprendre les enjeux et les contraintes potentielles.

3.1 Présentation du projet

Avec l'évolution des techniques de communication, les systèmes d'information et réseaux informatiques sont aujourd'hui de plus en plus ouverts sur le monde extérieur notamment avec Internet. Cette ouverture facilite la vie pour l'humain en lui offrant divers services, et relie des centaines de millions de machines à Internet un peu partout dans le monde. Cependant, cette interconnexion des machines permet également aux utilisateurs malveillants d'utiliser ces ressources et profiter de ses vulnérabilités à des fins abusives, par exemple : rendre un service web hors ligne.

La sécurité de nos jours est un problème d'une importance capitale, elle est devenue un problème majeur dans la gestion des réseaux d'entreprises ainsi que pour les particuliers. Différents mécanismes ont été mis en place pour faire face à ces problèmes de sécurité, comme les antivirus, les pares-feux, le cryptage, mais ces mécanismes ont des limites face au développement rapide des techniques de piratage. Pour éviter ces limites, l'utilisation des systèmes de détection d'intrusion s'impose.

Les systèmes de détection d'intrusions ont été conçus pour une surveillance continue, et la découverte des violations de la politique de sécurité, ainsi l'identification de toute activité non autorisée dans un réseau. Les pots de miel quant' à eux sont utiliser pour tromper les pirates afin de recueillir les informations sur les modes d'actions dans le réseau. Le système distribué permet le partage des informations sur les attaques en temps réels dans les différents sites afin que les mesures soient prises pour contrer cela.

3.2 Problématique

IP-TELRA étant une jeune entreprise offrant des services par ailleurs les services de stockage en ligne chez certains de ces partenaires, il comporte un grand nombre de données pour la plupart confidentielle dont le piratage pourrait s'avérer fatale pour l'entreprise. Jusque-là, aucune étude n'a encore été menée en vue de garantir aux administrateurs de savoir exactement les types de données (offensifs ou non) qui transitent sur les installations du réseau ainsi que les types d'activités exécutées par les utilisateurs qui y sont connectés. Il ne faudrait pas toujours attendre que le drame ne se produit avant de prendre des mesures correctives. La sécurité se doit d'être préventive au maximum afin de pouvoir éviter les éventuelles menaces. Le risque de zéro n'existant pas en matière de sécurité, nous pouvons tout de même s'y rapprocher en mettant en place un bon système de sécurité. Il est donc nécessaire de proposer au réseau un environnement de contrôle des types d'activités (offensif ou non) qui s'y opèrent. Aussi, est-il important de disposer d'un espace d'étude des attaques qui viseraient les équipements du réseau. Cela permettra aux administrateurs du réseau de suivre les nouvelles failles exploitées par les pirates ainsi que les nouveaux outils d'hacking.

3.3 Méthodologie et choix techniques

Notre proposition nécessite l'utilisation de plusieurs outils notamment les systèmes de détection d'intrusions (IDS) et les pots de miel. Nous présentons ici notre méthodologie de travail et les choix techniques opérés.

3.3.1 Méthodologie de travail

Ce travail se focalise sur les réseaux de grande étendue de façon générale et IP-TELRA en particulier. Dans ce réseau, nous distinguons les réseaux clients d'IP-TELRA et les infrastructures privées (serveurs de services et équipements réseaux) du réseau lui-même. Ainsi, il est nécessaire de procéder à l'analyse des données sur chaque site du réseau. Pour cela, nous étudions les systèmes de détection d'intrusions en vue de choisir le système le plus approprié selon nos objectifs notamment la communication entre instances autonomes. Ce choix nous permet de former notre environnement distribué sur tout le réseau. Ensuite, nous proposons l'espace d'étude des stratégies, des outils et des commandes utilisés par les pirates, en vue de

chaque fois adapter la politique de sécurité de tout le réseau aux nouvelles tendances de menaces. Il s'agit précisément d'un réseau de pots de miel. Nous analysons donc les types de pots de miel ainsi que les technologies de déploiement de honeynet (réseau de pots de miel) dans le but d'offrir le meilleur environnement possible. L'étape finale est consacrée aux différents tests afin de valider nos différentes propositions.

3.3.2 Choix du système de détection d'intrusion

Il existe différents systèmes de détection d'intrusions avec différentes caractéristiques que nous avons étudiés au chapitre 3. Pour la surveillance de chaque site client d'IP-TELRA, nous utilisons un système de détection d'intrusions réseau. Les IDS réseau sont plus appropriés en ce sens qu'ils ne nécessitent non seulement pas de toucher les machines déjà en production mais aussi permettent de surveiller tout un ensemble de machines à partir d'un point unique. C'est donc une technologie moindre coût nécessitant moins de ressources. De plus, ils ne surchargent pas le réseau et permettent une gestion plus facile de la maintenance. Dans la littérature, les outils les plus évolués pouvant permettre de réaliser cette fonction sont Snort, Suricata et Bro. Notre approche se base sur une architecture distribuée avec des agents complètement autonomes. Dans cette architecture, nous établissons des communications entre les différents agents. Donc, le NIDS doit nous permettre d'implémenter cela. Ainsi, Bro s'est révélé comme l'outil de choix. Comparativement à ces concurrents direct, Bro est nettement une technologie plus avancée. Il donne la possibilité de le personnaliser selon les objectifs désirés. Il est flexible avec un langage incorporé pouvant permettre de créer toute sorte d'outils réseau.

3.3.3 Taches effectuées par Bro (Zeek)

Zeek effectue deux tâches clés qui profitent aux organisations de sécurité :

1) Convertit les données sur le trafic réseau en événements de niveau supérieur ;

2) Fournit un interpréteur de script, un langage de programmation robuste qui est utilisé pour interagir avec les événements et comprendre ce que ces événements signifient en termes de sécurité du réseau.

En d'autres termes, Zeek capture des métadonnées sur l'activité sur un réseau, puis fournit un langage de programmation pour comprendre quand cette activité présente des indications malveillantes ou suspectes.

3.3.4 Bro par rapport aux IDS conventionnels

Lorsque Bro (Zeek) surveille un flux de trafic, il produit des journaux qui enregistrent tout ce qu'il comprend de l'activité du réseau. Cette compréhension inclut les enregistrements de connexion, le volume de paquets envoyés et reçus, les attributs des sessions TCP et d'autres métadonnées utiles pour analyser le comportement du réseau et comprendre le contexte de ce comportement.

Qu'est-ce qui est considéré comme un comportement réseau suspect dans une organisation, peut-être routinier dans une autre ? C'est pourquoi le langage de programmation Bro (Zeek) est si avantageux ; il peut être utilisé pour personnaliser l'interprétation des métadonnées aux besoins spécifiques d'une organisation.

Bro (Zeek) fournit un moyen d'effectuer les mêmes types de vérifications pour les attributs de trafic, mais avec la valeur ajoutée d'une interface de programmation. Cela signifie que Bro (Zeek) peut être utilisé pour calculer des statistiques numériques et des correspondances de modèles d'expressions régulières. Il peut également créer des conditions logiques complexes à l'aide des opérateurs AND, OR et NOT, qui permettent aux utilisateurs de personnaliser l'analyse en fonction de leur environnement.

3.3.5 Spécification de déploiement de Bro

Le déploiement de Bro dépend fortement de la politique de sécurité adoptée par l’organisation. Placé derrière un pare-feu externe, cette configuration permet à Bro de ne recevoir que des paquets filtrés conformément aux règles définies dans le pare-feu. Cela donne lieu à moins de notifications. Néanmoins certaines organisations préfèrent l’installer sans ce pare-feu dans le but de se voir notifier toutes les tentatives d’attaques. Une autre option est de le placer derrière le pare-feu interne lui permettant de détecter les machines internes infectées par les virus et les vers.

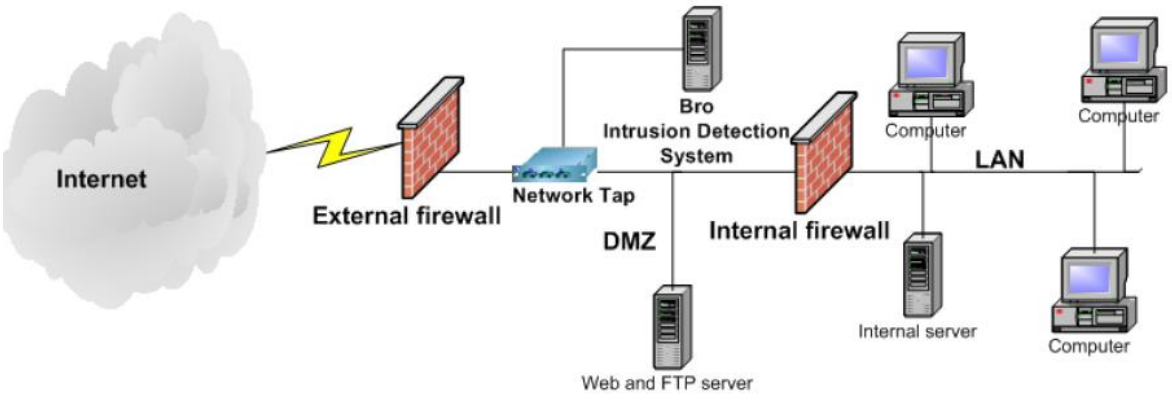


Figure 27 : Localisation typique d'un capteur et du système Bro

Bro ne requiert pas une machine spécialisée, et peut bien fonctionner sur une machine bon marché. Cependant le système doit contrôler tous les paquets entrant et sortant du site. Ainsi suivant le trafic réseau, il peut être nécessaire d'employer une machine assez robuste.

Le tableau suivant donne un récapitulatif des besoins requis pour le déploiement de Bro selon les caractéristiques du réseau de l'hôte.

Tableau 6 : Spécification des besoins de Bro

Nom	**Valeur**
Processeur	CPU à 1 GHz pour 100 Mbps avec un taux moyen de transfert <=5000 paquets/seconde CPU à 2 GHz pour 1 Gbps avec un taux <= 10000 paquets/seconde CPU à 3 GHz pour 1 Gbps avec un taux <= 20000 paquets/seconde CPU à 4 GHz pour 1 Gbps avec un taux <= 50000 paquets/seconde
OS	Le système recommandé est le FreeBSD. Bro peut bien tourner sur les systèmes de type Unix tels que Linux et solaris mais a été développé à l'origine pour le FreeBSD.
Mémoire	2 GB suffit pour un petit réseau (200 machines sur une connexion 100 Mbps). Pour un réseau plus grand, 4 GB de RAM sera nécessaire, avec 8-16 GB c'est encore mieux

Disque dur	20 GB minimum, 50 GB ou plus pour les logs est recommandé
Droit d'utilisateur	Requiert les droits administrateurs pour l'installation, puis lancé avec l'utilisateur Bro
Interfaces réseau	3 interfaces sont recommandées : 2 pour la capture de données (une par direction), et une pour la gestion de la machine. On pourrait utiliser la même interface pour les deux directions.
Autres	Perl version 5.6 ou plus (pour la génération de rapport) Libpcap version 0.7.2 ou plus

3.3.6 Utilisation des pots de miel

Comme nous l'avons souligné au chapitre 2, il existe les pots de miel basse interaction, moyenne et haute interaction. Les pots de miel haute interaction sont généralement utilisés dans les environnements de recherche dans le but de collecter des informations sur les pirates, leurs outils, leurs stratégies et leur comportement quand ils veulent prendre le contrôle d'une machine. Ces informations recueillies permettent par la suite de détecter les faiblesses puis de renforcer les outils de sécurité existants ou même d'en proposer de nouveaux. Ils sont beaucoup plus difficiles à gérer et posent de fortes contraintes de sécurité. De même les pots de miel à moyenne interaction ont pratiquement les mêmes exigences que ceux à haute interaction. En effet, ils ne sont qu'un compromis entre les deux autres mais généralement utilisés pour les mêmes objectifs que les précédents.

Par contre les pots de miel basse interaction sont beaucoup moins contraignants et le risque lié à leur utilisation est moindre. Ils émulent des services pouvant dialoguer avec les pirates sans pour autant leur offrir tant de liberté sur la machine. Dans un environnement de production, ils servent à détecter la présence effective de ces intrus dans le réseau tout en fournissant des informations utiles à leur sujet.

Notre objectif de vouloir étudier les attaques qui viseraient les serveurs en production sur le réseau nous impose l'utilisation des pots de miel haute interaction. Précisément nous formons un réseau de pots de miel afin de reproduire l'environnement de production. Cet environnement reproduit permet d'étudier les actions des pirates avec le réseau. Nous allons ainsi découvrir les trous possibles par lesquels les attaquants peuvent pénétrer le réseau.

Également l'analyse minutieuse des données permettra de découvrir les nouvelles attaques basées sur des techniques ou vulnérabilités nouvelles.

Il existe deux grandes générations de honeynet (réseau de pots de miel) : les honeynets de 1ere et 2e génération.

3.3.6.1 Les honeynets de 1ere génération

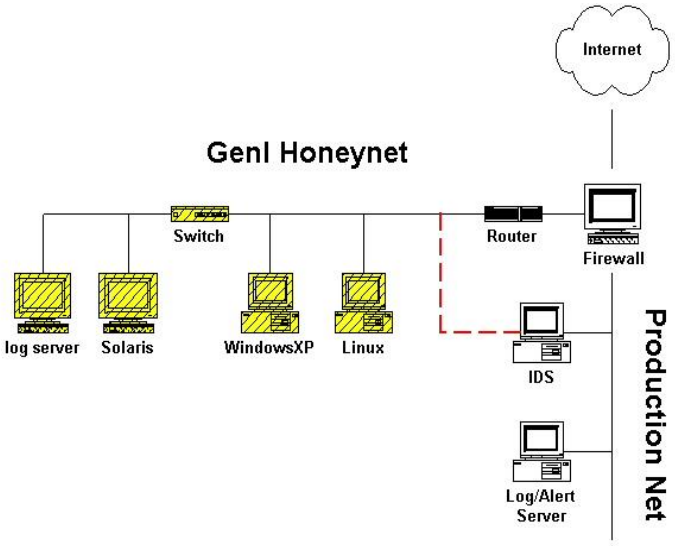


Figure 28 : Architecture honeynet de 1ère génération

La figure précédente présente l'architecture du honeynet de 1ere génération. Dans cette architecture, le réseau de pots de miel est complètement séparé du réseau de production à l'aide d'un routeur. Le contrôle de données est assuré par un pare-feu. Ce dernier compte le nombre de connexions initiées vers l'extérieur par le pirate quand il a pris le contrôle d'une machine du honeynet. Lorsque ce nombre atteint un seuil, le pare-feu bloque toute autre connexion sortante. Ainsi, on arrive à limiter les dégâts pouvant résulter des actions du pirate à l'extérieur. Par ailleurs, le pare-feu alerte lorsqu'il détecte une connexion à l'endroit du honeynet. Le routeur constitue aussi un point de contrôle de données. On peut notamment appliquer là des règles permettant de bloquer les ports généralement explorés par les pirates. Aussi peut-on filtrer les attaques par déni de services. La capture de données est réalisée par le pare-feu, un IDS et le honeypot compromis. Le pare-feu enregistre les adresses source et destination, les ports source et destination ainsi que le protocole utilisé. C'est une première couche de données très utile pour une analyse rapide des éléments engagés dans une communication. L'IDS stocke l'entièreté des paquets échangés avec le honeynet. Le honeypot compromis enregistre au niveau système ses conversations. Par ailleurs, il envoie ses logs vers un serveur spécial, ici log server

qui garde ces données de façon sécurisée. Cela permet donc d'isoler les logs du honeypot afin d'éviter qu'un pirate expérimenté ne les corrompe. En outre, une version modifiée de bash a été utilisée pour enregistrer discrètement les commandes tapées par le pirate.

Les grands défauts de cette architecture sont fortement liés aux connexions initiées par un honeypot et le pare-feu de couche 3 du modèle OSI. En effet, les 10 connexions tolérées sont largement suffisantes pour que de grands dommages soient causés par le pirate à l'extérieur. Aussi, cette limitation est un indice de fingerprinting. Le pirate peut se baser sur cette caractéristique pour s'apercevoir qu'il se trouve dans un honeynet. Dans ce cas les informations collectées ne sont plus crédibles car le pirate peut tout modifier et laisser de fausses données ou même en supprimer.

3.3.6.2 Honeynets de 2e génération

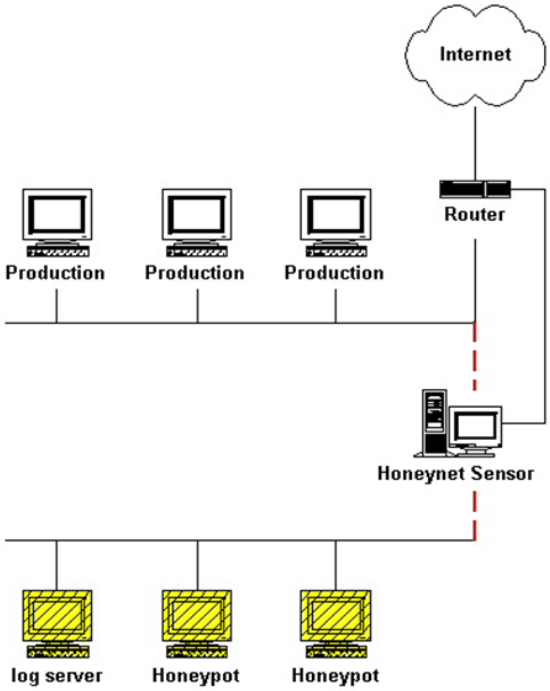


Figure 29 : Architecture honeynet de 2e génération

L'architecture des honeynets de 2e génération se présente comme à la figure précedente. Cette architecture est simple et difficile à détecter. En effet, deux équipements (le pare-feu et l'IDS) de la 1ere génération ont été fusionnés en un, le honeynet sensor (honeywall). Il réalise les fonctions des deux éléments précédents. Il fonctionne à la couche 2 de OSI. Cela offre un double avantage. Premièrement, il permet de réaliser le honeynet comme étant une partie du réseau comportant les serveurs de production et non de l'isoler complètement à l'aide d'un

routeur comme dans la 1ere génération. La séparation entre les deux réseaux est alors configurée au niveau 2 de OSI. Deuxièmement, il est difficile à détecter car fonctionnant à la couche 2. Il n'intervient donc pas dans le routage des paquets ; par conséquent aucun TTL n'est décrémenté et sa présence est discrète. Trois interfaces réseau sont utilisées : deux reliées à chacun des deux réseaux et une troisième directement connectée à internet pour la maintenance et la collecte dans le cas de honeynets distribués.

Sur la base de toutes ces informations, nous proposons de réaliser un honeynet de 2e génération afin d'offrir un environnement efficient, discret et évolutif.

3.4 Architectures proposées et principe de fonctionnement

Pour former l'architecture, il est nécessaire de déployer Bro sur chacun des sites du réseau et dans le data center. A cela s'ajoute un honeynet destiné à l'étude des attaques. Dans cette partie, nous présentons les différentes architectures de nos propositions ainsi que le principe de fonctionnement.

3.4.1 Mise en œuvre de Bro IDS

3.4.1.1 Localisation typique de Bro sur un site

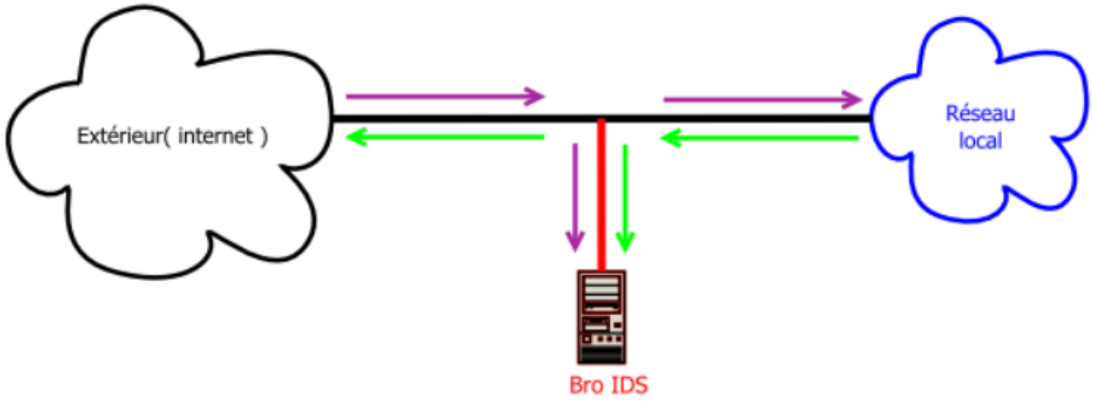


Figure 30 : Déploiement local de Bro

Bro est l'outil de détection d'intrusions que nous avons choisi d'utiliser. Ainsi, il est nécessaire de le déployer sur chacun des sites du réseau IP-TELRA. La figure ci-dessus présente sa localisation précise sur chaque site. C'est un positionnement typique qui lui permet de récupérer tout paquet entrant ou sortant du réseau interne. Notons que cette même configuration

est valable pour la surveillance des différents segments réseau du data center. L'essentiel est de disposer Bro de façon à ce qu'il reçoive tout échange du réseau. Il analyse donc tout le trafic du réseau.

3.4.1.2 Architecture de déploiement impliquant plusieurs sites

Comme souligné précédemment, la configuration précédente se répète sur chacun des sites de façon indépendante. Chaque instance Bro est configurée selon la politique adoptée sur le réseau local surveillé. Cependant une politique globale du réseau IP-TELRA nécessite une communication entre les différentes instances. Nous illustrons ce fonctionnement par l'architecture présentée à la figure ci-dessous. Notons que nous n'impliquons que trois sites pour illustrer la logique car en réalité plus nombreux sont les sites. Toutes les instances sont autonomes dans l'architecture. Donc la disparition d'une instance quelconque n'affecte pas le fonctionnement des autres. L'avantage principal de cette architecture est l'indépendance entre les instances, combinée avec la collaboration qu'elles réalisent entre elles. Cela est important en ce sens qu'il permet non seulement de définir la politique d'un site de façon presque indépendante des autres mais aussi de définir une politique globale du réseau. Cela peut être vu comme une combinaison des architectures basées sur des agents autonomes et celles utilisant des capteurs distribués autour d'une entité centrale, sauf que nous n'avons pas prévu ici une unité centralisée de gestion.

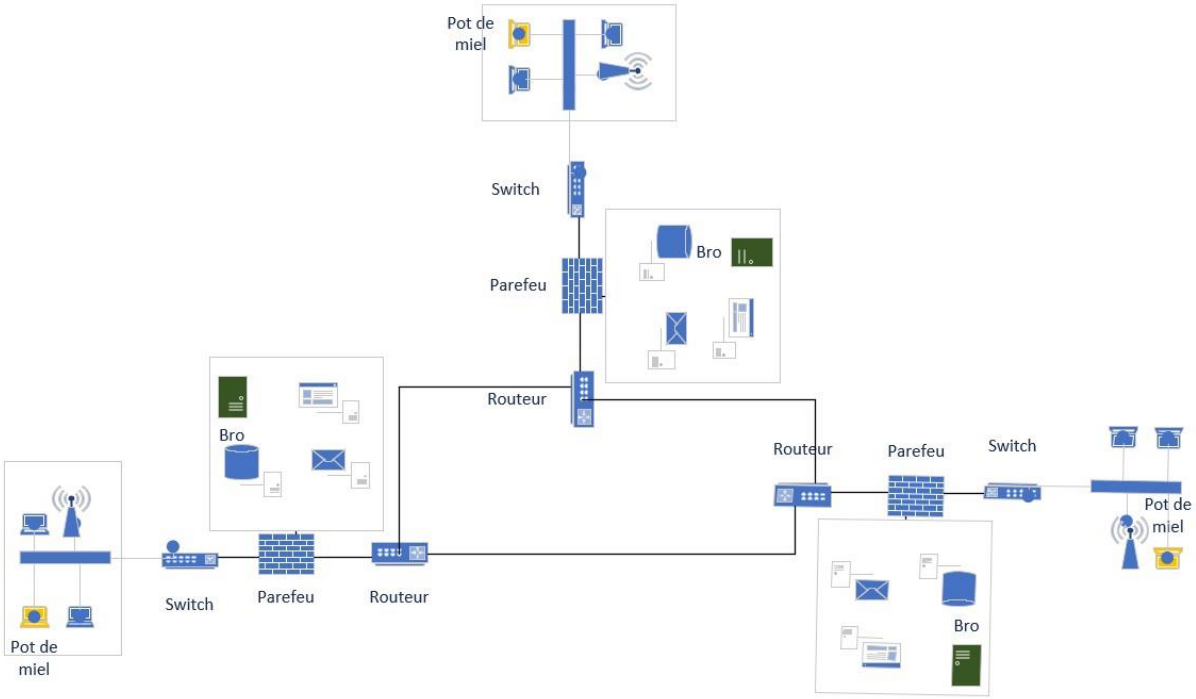


Figure 31 : Architecture impliquant plusieurs sites

Conclusion partielle

Cette partie nous a ainsi permit de définir méthodologie de travail et de pouvoir trouver des solutions qui conviennent à son besoin. Il est donc question pour nous maintenant de faire un cahier de charge qui nous servira à l'élaboration du projet proprement dit. Notre prochain chapitre sera donc ici l'élaboration du cahier de charge.

Chapitre 4 : Cahier des charges

Le cahier des charges définit clairement et de manière complète l'intervention de formation à mettre en place. Il décrit très précisément les modalités d'exécution, le cadre… En interne, il sert à les expliquer aux différents acteurs et à s'assurer que tout le monde est d'accord, qu'il y a bien eu concertation.

4 Cahiers des charges

4.1 Introduction

Le cahier des charges est un document contractuel établit entre le maître d'œuvre et le maître d'ouvrage qui étale les besoins du client. Il joue le rôle d'étude et de présentation avec exactitude des exigences formulées par les utilisateurs en ce qui concerne le projet, son déroulement et les résultats attendus. Le présent cahier des charges traite de l'élaboration d'un système de détection et prévention d'intrusions à partir de capteurs distribués dans un réseau informatique plus précisément le réseau informatique de l'entreprise IP-TELRA.

4.2 Société

4.2.1 Présentation de l'entreprise

Située au cœur de Douala, notre Société à taille humaine, créée en 2013 est une SSII (société de services en ingénierie informatique) / ESN (entreprise de services du numérique) spécialisée dans les services informatiques et la transformation numérique (maintenance, infogérance, sécurité informatique et services Cloud), s'adressent aussi bien aux TPE, PME/PMI, aux collectivités et administrations publiques, au secteur de l'éducation et de la santé sensibles à la notion de qualité de service.

Fidèle à ses valeurs de services, IP-TELRA privilégie la qualité de ses prestations, la fiabilité et la réactivité de ses équipes commerciales et techniques ainsi que la disponibilité de son support technique.

Figure 32: Logo IP-TELRA

4.2.2 Localisation

L'entreprise IP-TELRA est située à Makepé au niveau du carrefour lycée DOUALA - CAMEROUN - (+237) 693 055 513 / 672 574 654

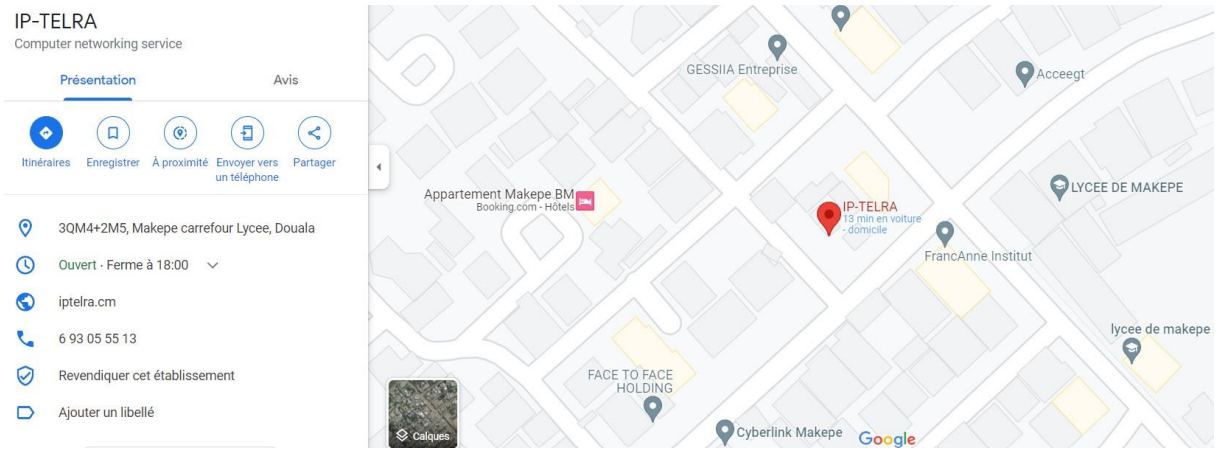


Figure 33: Localisation IP-TELRA

4.2.3 Activité

Un objectif clair : Accompagner nos Clients dans la réflexion, la réalisation, l'évolution et le suivi de l'ensemble de leur système d'information tout en respectant les valeurs essentielles que nous défendons : professionnalisme, compétitivité, disponibilité et réactivité mais surtout respect du Client et des engagements.

IP-TELRA apporte des solutions et services agiles pour votre système d'information et votre transformation numérique !

- Audit, conseil, helpdesk & ingénierie IT
- Maintenance et Infogérance système
- Réseau & sécurité informatique
- Intégrateur d'infrastructures IT
- Hébergement & cloud computing
- Développement Web et digital

L'IT au cœur de votre activité

- Infogérance & Supervision

- Helpdesk
- Délégation de ressources
- Electricité
- Formation
- Télécom

4.2.4 Chiffres-clés

Pour un capital d'ouverture de 42 millions de franc CFA à sa création en 2013, à ce jour l'entreprise IP-TELRA réalise un chiffre d'affaire d'environ 18 millions de franc par an.

4.2.5 Réalisation

Une SSII au cœur de votre activité

- Externalisation SI
- Sécurité & réseau
- Messagerie & Collaboration
- Vidéo surveillance
- Interactivité & collaboration
- Leasing
- Virtualisation
- Sauvegarde en ligne
- Téléphonie IP
- Affichage dynamique
- Couverture Wifi
- Connectivité / Liens

4.3 Présentation du projet

4.3.1 Contexte du projet

L'augmentation des attaques et la complexité de celles-ci compliquent de plus en plus la mise en place et la gestion des réseaux. En effet, il est nécessaire de garantir la disponibilité

de chaque équipement du réseau. De la même manière l'intégrité et la confidentialité des données constituent un enjeu important. Les attaques informatiques peuvent se retrouver sous plusieurs formes à savoir virus, vers, chevaux de Troie et autres. Cette variété déjoue presque toujours, tôt ou tard, les moyens de sécurité, justifiant largement la locution "le risque zéro n'existe pas". De nouveaux outils sont inventés, de nouveaux concepts apparaissent, de nouvelles politiques de sécurité sont implémentées sans pour autant offrir une sécurité entière aux systèmes d'information. Ainsi, malgré toutes les stratégies de sécurité, les menaces n'ont jamais cessé d'exister. Tout réseau ouvert à d'autres réseaux est alors sous menace permanente.

4.3.2 Justification du projet

IP-TELRA bien qu'étant un réseau fédérateur, jusque-là n'a encore été menée aucune étude en vue de garantir aux administrateurs de savoir exactement les types de données (offensifs ou non) qui transitent sur les installations du réseau ainsi que les types d'activités exécutées par les utilisateurs qui y sont connectés. Il est donc nécessaire de proposer au réseau un environnement de contrôle des types d'activités (offensif ou non) qui s'y opèrent. Aussi, est-il important de disposer d'un espace d'étude des attaques qui viseraient les équipements du réseau. Cela permettra aux administrateurs du réseau de suivre les nouvelles failles exploitées par les pirates ainsi que les nouveaux outils d'hacking.

4.3.3 Objectifs du projet

a. Objectif principal

L'objectif principal qui nous guide dans ce travail est de proposer une architecture distribuée de détection et de prévention d'intrusions basée sur l'utilisation de systèmes de détection d'intrusions. Nous proposons également un réseau de pots de miel dont le but est d'étudier les menaces contre IP-TELRA, afin de chaque fois réadapter la politique implémentée dans les systèmes de détection contre les nouvelles tendances de menaces.

4.3.3.1 Objectifs spécifiques

Pour arriver a bien dans notre travail nous devrons :

- ✓ Installer Bro IDS pour le filtrage des paquets ;
- ✓ Créer des règles de filtrage pour sécuriser de réseau ;

- ✓ Installer un ordinateur pot de miel pour tromper les attaquants ;
- ✓ Faire communiquer les différents équipements dans le réseau ;
- ✓ Mettre en place un réseau d'IDS distribué ;
- ✓ Centralisez les alertes liés aux incidents de sécurité ;
- ✓ Envoyer des alertes si l'analyse montre qu'une activité s'exécute sur des ensembles de règles prédéterminées, comme par exemple l'exécution d'un logiciel malveillant, et indique ainsi un problème de sécurité potentiel.

4.3.4 Périmètre du projet

Le présent projet s'étant au niveau de l'ensemble du réseau informatique de la structure lié à internet afin de garantir la sécurité du trafic des données et des entités communiquant via le réseau internet.

4.4 Expression des besoins

L'expression des besoins est une étape dans un projet permettant de définir tout ce que l'on souhaite en ressortant tout ce qui est obligatoire, fonctionnel et non fonctionnel. En outre, dans cette partie, nous définissons précisément quelles sont les fonctions attendues par IP-TELRA ; qu'est-ce qui sera fait dans le projet, d'un point de vue fonctionnel et non fonctionnel.

4.4.1 Besoins fonctionnels

- Possibilité d'analyser des données et le trafic dans le réseau ;
- Possibilité de filtrer les paquets ;
- Possibilité de configurer et de mettre ajour les règles de filtrage ;
- Possibilité de bloquer les menaces ;
- Possibilité de manager le trafic ;
- Possibilité de tromper les cybers attaquants ;
- Possibilité de recueillir les informations sur les attaques et les attaquants ;
- Possibilité d'ajuster les règles de filtrage et définir les nouvelles mesures de protections;

- Possibilité de mettre en liaisons les différents sites ;
- Possibilité de partager les informations entre les sites ;
- Possibilité de manager l'ensemble des sites ;
- Possibilité de centraliser les informations sur les attaques et les menaces entres les différents sites ;
- Possibilité d'apporter des mesures préventives et correctives face aux menaces.

4.4.2 Besoins non fonctionnels

- L'**intégrité** : « L'intégrité est la prévention d'une modification non autorisée de l'information » c'est-à-dire de l'information doit être transmise dans sa valeur réelle sans être modifié ou même déformé norme ISO 7498-2 (ISO90) ;
- La **haute disponibilité :** Propriété d'accessibilité au moment voulu des données et des fonctions par les utilisateurs autorisés ;
- La **maintenabilité :** elle devra être maintenue dans la facilité totale ;
- La **rapidité du traitement** : L'accès aux données et les filtrages des paquets doivent être spontanée. En aucun moment cela ne doit ralentir le travail des utilisateurs et les services de l'entreprise.
- L'**évolutivité** : L'infrastructure doit permettre d'intégrer facilement de nouveaux serveurs pour améliorer la qualité de service sans pour autant devoir repenser le système. Par exemple on doit pouvoir ajouter un nouveau site sans pour autant repenser l'architecture de zéro.
- La **redondance des données** : Toutes les données nécessaires au bon fonctionnement de la plateforme devront être dupliquées afin de ne perdre le minimum en cas de défaillance d'un serveur ou d'un service.

4.5 Les ressources du projet

La réalisation du dit projet fait intervenir diverses ressources.

4.5.1 Ressources matérielles

Le tableau suivant présente l'ensemble des matériaux dont nous aurons besoin pour la réalisation de notre projet.

Tableau 7: Ressources matérielles du projet

Nom du matériel	**Propriété**
Ordinateur portable DELL	Processeur cor i5 4ème génération fréquence 1.70 Ghz x 4 Disque dur SSD SATA 128 giga Ram 12 giga
Ordinateur portable HP	Processeur cor i7 4ème génération fréquence 2.40 Ghz x 4 Disque dur SSD M2 SATA 128 giga Ram 16 giga
Mini routeur TP-LINK	Model TL-WR740N Vitesse de transfert 150Megabits/seconde

4.5.2 Ressources logicielles

Nous avons ici l'ensemble de logiciels nécessaire à la conception et à la réalisation de notre projet.

Tableau 8: Ressources logicielles du projet

Nom du logiciel	**Utilisation**	**Taille**	**Version**	**Éditeur**
Google chrome	Navigateur web	75.1Mo	5.0.4183.8	**Google Inc.**
GANTT PROJECT	Outil d'aide à la planification des projets	22 Mo	2.0.10	**Free Software Fondation**

Windows 10	Interface homme-machine	5 Go	1703	**Microsoft**
Microsoft office professionnel plus 2019	Edition des documents & rapports & architecture	1,18 Go	2008 build 13127.20616	**Microsoft**
Microsoft Visio professionnel 2019	Conception des architectures	3.47Go	2008 build 13127.20616	**Microsoft**
Kali linux	Système d'exploitation	4,6GO	2021.2	**Offensive Security,**
Oracle VM Virtualbox	Hyperviseur	16 Mo	6.1.12	**Oracle Corporations**
Metasploit	Outils de pentest	212 Mo	4.19	**Rapid7 LLC**
Wireshark	Analyseur de paquet	56,4 Mo	3.4.7	**Projet Wireshark**
Nmap	Scanner de port	26,01 Mo	7.92	**Fyodor**
Bro	Sonde de détection d'intrusions réseau (NIDS)	/	2.4.1	**Lawrence Berkeley National Laboratory**
Pot de miel	Trompeur d'attaquant	/	2.5.6	**/**
Ubuntu serveur	Système d'exploitation serveur	/	22.04	**Canonical Ltd**

4.5.3 Ressources humaines

Les ressources humaines représentent les personnes qui vont intervenir dans notre projet, les acteurs de notre projet. Le tableau suivant présente l'ensemble des intervenants du projet.

Tableau 9: Ressources humaines du projet

Personnes en	Titres	Rôles
M. TIOWA NZONTEU	Expert réseau, infrastructure et sécurité	Charger de faire l'étude et la mise en place de la solution. De configurer la solution et de l'intégrer au réseau d'IP-TELRA
M. NANA TCHOFFO Michel	Ingénieur en maintenance des systèmes informatique	Charger de la supervision et de la maintenance du système après son déploiement
M. TCHOFFO Guy	Ingénieur des réseaux et télécom	Charger de former et de mettre en place l'équipe qui exploitera la solution

4.6 Estimations financières

Le tableau suivant présente une évaluation financière du projet dans sa globalité.

Tableau 10: Estimation financière du projet

Libellé	Quantité	P.U (en FCFA)	Montant
Matériels informatiques			
Ordinateur portable DELL	01	180 000	**180 000**
Ordinateur portable HP	01	230 000	**230 000**
Mini routeur TP-LINK	01	45 000	**45 000**
Total		455 000	
Logiciels			
Google chrome	01	Gratuit	/
GANTT PROJECT	01	Gratuit	/
Windows 10	01	138 000	**138 000**
Microsoft office professionnel plus 2019	01	188 500	**188 500**
Microsoft Visio professionnel	01	70 850	**70 850**

Kali linux	01	Gratuit	/
Oracle VM VirtualBox	01	Gratuit	/
Metasploit	01	Gratuit	/
Wireshark	01	Gratuit	/
Nmap	01	Gratuit	/
Ubuntu serveur	01	Gratuit	/
Bro NIDS	01	Gratuit	/
Pot de miel	01	Gratuit	/
Total		397 350	
Rémunérations			
Ingénieur ERIS	01	70 850/j (sur 15 jours)	**1.062.750**
Ingénieur MSI	01	56 000/j (sur 5 jours)	**280 000**
Ingénieur réseau et télécom	01	62 170/j (sur 5 jours)	**310 850**
Total		1 653 600	
Divers			
Accès à internet	24h/24	25 000/30 jours	**25 000**
Total		**25 000**	
Risque du projet			
Forfait (20% du coût total)	Coût total du projet sans risque 2 530 950		**Total forfait 506 190**
Montant final du projet		**3 037 140 FCFA**	

Cette estimation a été faite à l'aide de **la méthode de calcul des coûts spécifiques** [13]

- Principe

Cette méthode intègre dans son calcul toutes les charges directes, variables ou fixes. Elle ne prend pas en compte les éléments indirects, intégrés dans les coûts de structure. L'objectif est de faire ressortir une marge sur coût spécifique.

- Intérêt

Il s'agit d'un indicateur très opérationnel pour juger la rentabilité d'un produit en évaluant la valeur créée. Il est ainsi possible de décider le maintien ou l'arrêt de sa commercialisation.

4.7 Planification du projet

Planifier notre projet implique d'effectuer une répartition des tâches sur une durée de trois semaines c'est-à-dire 15 jours tel que présenté sur le diagramme de Gantt ci-dessous.

4.7.1 Planification des tâches

Cette planification est effectuée sur une durée d'une semaine telle que représente le tableau suivant :

Tableau 11: Planification des taches du projet.

Responsables	Tâches	Résultats attendus	Durée
Ingénieur ERIS	Élaboration de la charte du projet	Plan de management du contenue et des exigences du projet	**3 jours**
	Identification des parties		
	Recueil des exigences		
	Élaboration du contenu du projet		
	Découpage du projet		
	Identification des risques	Plan de management des risques	**4 jours**
	Analyse qualitative et quantitative des risques		
	Classification des risques		
	Solution aux risques		
	Identification des menaces, des risques et l'impact sur le système		
	Mise sur pied de la solution	Solution de détection et prévention des risques	**3 jours**
	Configuration de la solution	Définition des règles et des scénarios	**2 jours**

	Intégration de la solution au système d'IP-TELRA	Déploiement de la solution	**3 jours**
Ingénieur MSI	Définition d'un plan de maintenance	Livrable plan de maintenance système	**2 jours**
	Gestion des maintenance système	Gestion des mises à jour et de la base de données	**3 jours**
Ingénieur Réseau et Télécom	Interconnexion des sites et gestion des stratégies réseaux	Communication inter sites	**2 jours**
	Formation des analystes	Document de formation et guide d'utilisation	**3 jours**

4.8 Planification sur Gantt

La planification du travail sur Gantt nous donne le résultat illustré par l'image suivante :

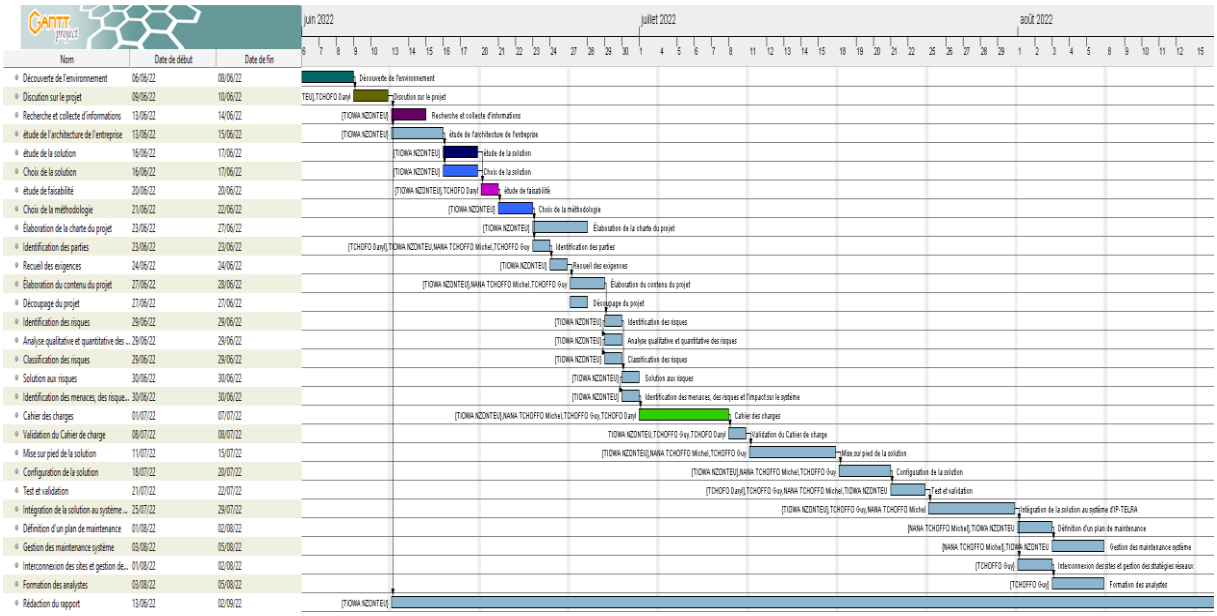


Figure 34: Planification du projet sur Gantt

4.9 Modalités / contraintes du projet

La conduite de ce projet de sécurité se basera sur trois contraintes essentielles qui sont :

- **Les contraintes sur coût :** Le budget fixé pour la conduite de ce projet devra être respecté conformément aux prévisions c'est-à-dire sans surenchère ou sous-enchère ;
- **Les contraintes sur le délai :** La réalisation de ce projet devra respecter les contraintes de temps fixés et donc être faite sur une durée précise et devra respecter les objectifs fixés ;
- **Les contraintes de qualités :** Nous réalisons une des missions les plus importantes qui soit en matière de sécurité. Le résultat attendu devra être intuitif, claire et sans ambiguïté.

4.10 Livrable

Il s'agit ici de ce qui est attendu à la fin de ce projet d'amélioration de la sécurité. Dans le cas présent, la livrable principale sera la documentation de la solution mise en place. Elle contiendra entre autres les détails sur les composantes de l'architecture, toutes les procédures ainsi que les recommandations pour le suivi et le maintien en condition opérationnel de la solution.

Conclusion partielle

Parvenue au terme de ce chapitre où il a été question pour nous de l'élaboration d'un cahier de charge pour le cadre de projet, nous avons eu à fixer les objectifs visés par la conception de ce système et dressé une liste des besoins conformément aux attentes d'IP-TELRA. Nous y avons également établi une étude financière du projet qui fait appel à la présentation des ressources humaines, matériels et logiciels nécessaires, ainsi qu'à une planification du projet sur une période bien déterminé dans le respect des contraintes de coût, de délai et de qualités.

Chapitre 5 : Implémentation et résultats

Le but de ce chapitre est de présenter comment les propositions des chapitres précédents sont mises en place. Plus précisément, il présente l'installation des outils et les configurations nécessaires à la mise en place de notre système de détection et de prévention d’intrusions à partir des capteurs distribués dans un réseau informatique.

5 Implémentation et résultats

L'implémentation est la réalisation, l'exécution ou la mise en pratique d'un plan, d'une méthode ou bien d'un concept, d'une idée, d'un modèle, d'une spécification, d'une norme ou d'une règle dans un but précis. L'implémentation est donc l'action qui doit suivre une réflexion pour la concrétiser. Alors dans ce chapitre nous allons présenter les installations de note solutions et les résultats obtenus.

5.1 Implémentation

5.1.1 Installation des prérequis

Il s'agit ici de l'installation de l'environnement de travail et des prérequis des différents systèmes d'exploitation.

Nous avons installé ici :

- Ubuntu server version 16.04 pour accueillir notre solution bro
- Une machine Kali pour les différents tests de vulnérabilité dans le réseau
- Un machine utilisateur Windows 10
- Une machine Ubuntu 20.04 pour le pot de miel

5.1.1.1 Prérequis pour la machine Ubuntu serveur bro

Installation des mises à jour système

sudo apt-get update && sudo apt-get full-upgrade

Installation des dépendances

```
root@Zeek:/home/zeek# apt-get install cmake make gcc g++ flex git bison python-dev swig libpcap-dev
libssl-dev zlib1g-dev
```

Figure 35: Installation des dépendances pour Bro

5.1.1.2 Prérequis pour le pot de miel

Mise à jour du système Ubuntu

sudo apt-get update && sudo apt-get full-upgrade

Installation des librairies et des dependances

apt-get install cmake make gcc g++ flex git bison python-dev swig libgeoip-dev libpcap-dev libssl-dev zlib1g-dev -ylibgeoip-dev -y

5.1.1.3 Configuration réseau des postes

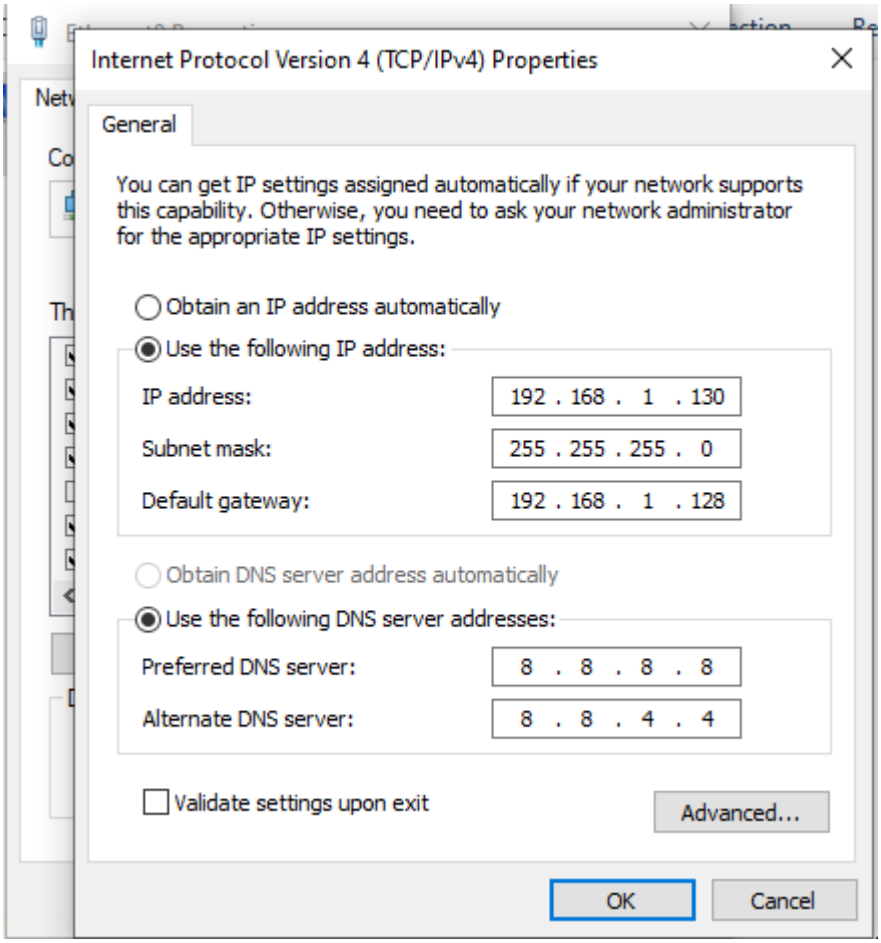


Figure 36: Configuration réseau du poste utilisateur

```
 GNU nano 2.5.3        Fichier : /etc/network/interfaces

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
auto ens33 inet static
address 192.168.1.129
netmask 255.255.255.0
gateway 192.168.1.128
dns-nameservers 8.8.8.8 8.8.4.4
```

Figure 37: Configuration réseau pour le pot de miel

```
root@Zeek:/opt/bro/logs/current# ls
communication.log  dns.log    known_hosts.log     software.log  stdout.log
conn.log           files.log  known_services.log  ssl.log       weird.log
dhcp.log           http.log   notice.log          stderr.log    x509.log
root@Zeek:/opt/bro/logs/current#
```

Figure 38: Configuration réseau pour le serveur Bro

5.1.2 Installation Bro NIDS

Téléchargement de la version 2.4.1 de bro

```
root@Zeek:/home/zeek# wget http:/www.bro.org/downloads/release/bro-2.4.1.tar.gz
```

Figure 39: Téléchargement de la version 2.4 de Bro

Décompression de bro du fichier de téléchargement de Bro

```
root@Zeek:/home/zeek# ls
bro-2.4.1.tar.gz
root@Zeek:/home/zeek# tar -xvzf bro-2.4.1.tar.gz
```

Figure 40: Décompression de Bro

Création d'un répertoire OPT et accès au fiches décompressé

```
root@Zeek:/home/zeek# cd bro-2.4.1
root@Zeek:/home/zeek/bro-2.4.1# mkdir /opt/bro
root@Zeek:/home/zeek/bro-2.4.1#
```

Figure 41: Création du répertoire OPT

Configuration du répertoire d'installation

```
root@Zeek:/home/zeek# cd bro-2.4.1
root@Zeek:/home/zeek/bro-2.4.1# mkdir /opt/bro
root@Zeek:/home/zeek/bro-2.4.1# ./configure --prefix=/opt/bro
```

Figure 42: Configuration du répertoire d'installation

Installation de bro dans le répertoire prédéfini

```
root@Zeek:/home/zeek/bro-2.4.1# make_
```

Figure 43: Initialisation de l'installation de bro

```
root@Zeek:/home/zeek/bro-2.4.1# make install_
```

Figure 44: Installation de bro dans le répertoire

Définition d'une variable d'environnement pour avoir accès à la bibliothèque bro dans le terminal d'autre système d'autre système

```
root@Zeek:/home/zeek/bro-2.4.1# export PATH=/opt/bro/bin:$PATH
```

Figure 45: Définition de la variable d'environnement

Editer le fichier de configuration de bro

```
root@Zeek:/home/zeek/bro-2.4.1# vim /opt/bro/etc/
broccoli.conf  broctl.cfg     networks.cfg   node.cfg
root@Zeek:/home/zeek/bro-2.4.1# vim /opt/bro/etc/node.cfg
```

Figure 46: Editer le fichier de configuration de bro

Configuration de bro pour l'accès au réseau local et configuration de l'interface de communication de bro ainsi que les réseaux que bro aura à écouter.

```
# Example BroControl node configuration.
#
# This example has a standalone node ready to go except for possibly changing
# the sniffing interface.

# This is a complete standalone configuration.  Most likely you will
# only need to change the interface.
[bro]
type=standalone
host=localhost
interface=ens33
```

Figure 47: Interface de communication réseau de bro

Figure 48: Définition du type d'adresse du réseau

Finalisation de l'installation

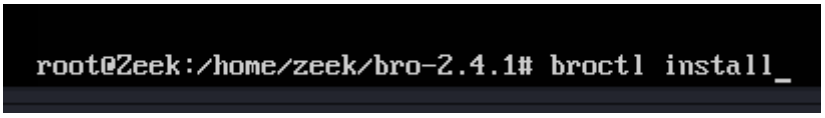


Figure 49: Finalisation de l'installation

Démarrage des services de bro

Figure 50: Démarrage des services de Bro

Statut de bro après installation

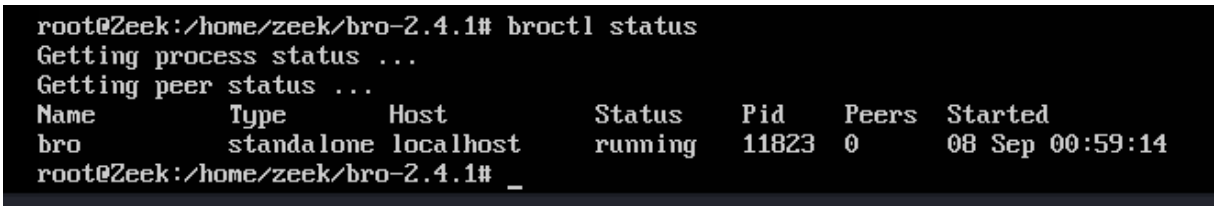


Figure 51: Présentation de Bro

Configuration des fonctions de routage de bro

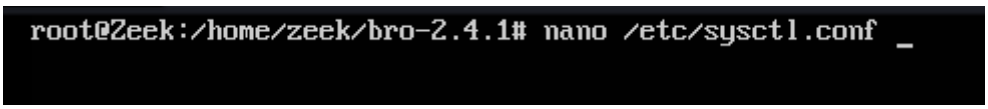


Figure 52: Fonction de routage de Bro

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Figure 53: Redistribution des paquets

```
root@Zeek:/home/zeek/bro-2.4.1# sysctl -p /etc/sysctl.conf
net.ipv4.ip_forward = 1
root@Zeek:/home/zeek/bro-2.4.1# _
```

Figure 54: Validation de la redistribution des paquets

```
root@Zeek:/home/zeek# ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:07:c7:ec
          inet adr:192.168.1.128  Bcast:192.168.1.255  Masque:255.255.255.0
          adr inet6: fe80::20c:29ff:fe07:c7ec/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Packets reçus:12 erreurs:0 :0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          Octets reçus:1544 (1.5 KB) Octets transmis:1962 (1.9 KB)

ens36     Link encap:Ethernet  HWaddr 00:0c:29:07:c7:f6
          inet adr:192.168.176.129  Bcast:192.168.176.255  Masque:255.255.255.
          adr inet6: fe80::20c:29ff:fe07:c7f6/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Packets reçus:224 erreurs:0 :0 overruns:0 frame:0
          TX packets:241 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          Octets reçus:61120 (61.1 KB) Octets transmis:19882 (19.8 KB)
```

Figure 55: Présentation des liens de redistribution des paquets

```
root@Zeek:/home/zeek# iptables -t nat -A POSTROUTING -o ens36 -j MASQUERADE
```

Figure 56: Activation de la fonction de routage

5.1.3 Installation des pots de miel

Installation des services SNMP et Samba, vous devrez installer les packages suivants.

$ sudo apt-get install -y python3-scapy # SNMP

$ sudo apt-get install -y samba # Samba

On crée un environnement virtuel pour installer OpenCanary. Il permettra de faire un cloisonnement.

$ sudo virtualenv honeypotenv/

. honeypotenv/bin/activate

On peut maintenant installer OpenCanary.

$ pip install opencanary

Pour utiliser le SNMP.

$ pip install scapy pcapy

Nous allons générer le fichier de configuration.

$ opencanaryd –copyconfig # il y a 2 “-“

Avant de modifier le fichier de configuration, nous allons faire une copie.

$ sudo cp /etc/opencanaryd/opencanary.conf

/etc/opencanaryd/opencanary.conf.svg

Nous allons maintenant modifier le fichier de configuration de OpenCanary.

$ sudo nano /etc/opencanaryd/opencanary.conf

Dans ce fichier de configuration, on peut voir l’ensemble des services que peut simuler OpenCanary.

Voici la description des champs :

- **device.node_id:** nom du serveur (évité de conserver celui par défaut ou de mettre honeypot)
- **ip.ignorelist:** permet de renseigner les ip considérées comme légitime (exemple : un scanner du vulnérabilité). Cela permet d’éviter de recevoir des alertes pour rien.
- **git:** permet d’être alerté en cas de clonage du repo git

- **ftp:** permet d'être alerté en cas de tentatives de connexion au serveur FTP
- **http:** permet d'être alerté en cas de tentatives de connexion au serveur Web
- **httpproxy:** permet d'être alerté en cas de tentatives de connexion au serveur proxy HTTP
- **portscan:** permet d'être alerté en cas de scan sur la machine
- **smb:** permet d'être alerté en cas de tentatives de connexion au serveur samba
- **mysql:** permet d'être alerté en cas de tentatives de connexion au serveur mysql
- **ssh:** permet d'être alerté en cas de tentatives de connexion en ssh au serveur (attention fonctionne si l'hôte n'a pas le ssh activé)
- **rdp:** permet d'être alerté en cas de tentatives de connexion en rdp au serveur
- **sip:** permet d'être alerté en cas de tentatives de connexion au serveur SIP
- **snmp:** permet d'être alerté en cas de requête sur les OID snmp
- **ntp:** permet d'être alerté en cas de requêtes ntp
- **tftp:** permet d'être alerté en cas de tentatives de connexion au serveur TFTP
- **tcpbanner:** permet d'être alerté en cas de tentatives de connexions et fourni les données reçus
- **telnet:** permet d'être alerté en cas de tentatives de connexion en telnet au serveur
- **mssql:** permet d'être alerté en cas de tentatives de connexion au serveur mssql
- vnc: permet d'être alerté en cas de tentatives de connexion au serveur VNC

5.2 Résultat

5.2.1 Test de fonctionnement de honeypot

Nous allons maintenant faire un test de fonctionnement. Sur notre serveur on va envoyer une requête http.

$ wget http://ip_du_serveur

Voici le message dans les logs (/var/tmp/opencanary.log).

Envoi des logs vers un collecteur

Si vous souhaitez envoyer les logs vers un collecteur, il faut modifier le fichier de configuration.

$ sudo nano /etc/opencanaryd/opencanary.conf

Puis on rajoute dans la section handlers

"json-tcp": {

"class": "opencanary.logger.SocketJSONHandler",

"host": "ip_serveur_log",

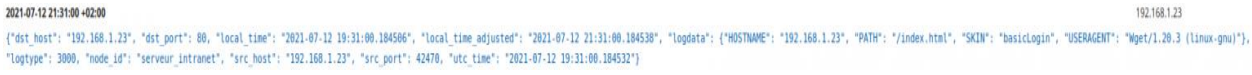
"port": 1514

},

```
"handlers": {
    "console": {
        "class": "logging.StreamHandler",
        "stream": "ext://sys.stdout"
    },
    "json-tcp":{
        "class": "opencanary.logger.SocketJSONHandler",
        "host": "192.168.1.106",
        "port": 1514
    },
    "file": {
        "class": "logging.FileHandler",
        "filename": "/var/tmp/opencanary.log"
    }
}
```

$ sudo systemctl restart opencanary.service

Maintenant nos logs sont bien envoyés vers le collecteur.



Pour l'extrator, le fichier de log est au format json, il suffit donc de créer un extrator au format json en laissant les paramètres par défaut.

CONCLUSION

La surveillance des données qui transitent sur un réseau permet non seulement de se protéger des menaces, mais aussi d'éviter d'être une zone de transit d'attaques. Dans ce projet, le but de notre travail était de mettre en place un système de détection et de prévention d'intrusion à l'aide des capteurs distribués dans un réseau à fin d'accroitre le niveau de sécurité de l'entreprise IP-TELRA, nous avons proposé de façon générale, une architecture distribuée de détection et de prévention d'intrusions basée sur des agents autonomes ; puis nous l'avons intégré à l'architecture du réseau IP-TELRA. Nous avons dans cette optique utilisé le NIDS Bro que nous avons déployé en tant qu'analyseur réseau sur chaque site. Chaque instance de l'architecture partage des événements avec les autres instances. Pour réaliser cela, nous avons développé en langage Bro deux scripts : sender.bro et receiver.bro. Ces scripts permettent donc d'établir la communication en les différents agents ainsi que les réactions à adopter lors de l'apparition de ces événements. En outre, nous avons proposé un réseau de pots de miel destiné à l'étude des attaques et outils de piratage. Les informations collectées dans cet espace permettront de suivre les vulnérabilités que les pirates pourraient exploiter dans le réseau IP-TELRA. En conséquence, les administrateurs devront adopter la réaction nécessaire pour réduire ces vulnérabilités.

Afin de pouvoir bénéficier des avantages d'une gestion centralisée, nous proposons comme perspective à ce travail, l'implémentation des mécanismes de collecte d'événements ou d'alertes vers une entité de gestion centrale. Nous aurions alors une architecture provenant d'une combinaison d'architecture distribuée basée sur des agents complètement autonomes et d'architecture distribuée centralisée. Aussi, avec les possibilités offertes par Bro, il serait utile d'instrumenter c'est-à-dire réécrire, à l'aide de Broccoli, les applications (SSH, HTTPS,etc) qui tournent sur les serveurs du honeynet pour qu'elles envoient à Bro, les données qu'elles ont effectivement reçues. Cela permettra par exemple de traquer les connexions cryptées qu'il n'est pas possible d'analyser au niveau réseau.

REFERENCES

[1] H. Kahina, «Implémentation d'un réseau VPN . Cas: Entreprise ENIEM,» Universite Mouloud MAMMERI Tizi-Ouzou, 14 Juillet 2015. [En ligne]. Available: https://www.ummto.dz/dspace/handle/ummto/12468. [Accès le 18 Juin 2022].

[2] l. n. d. T. (ANTIC), «cio-mag,» 09 Mars 2022. [En ligne]. Available: https://cio-mag.com/cybercriminalite-plus-de-12-milliards-de-fcfa-perdus-en-2021-risques-majeurs-au-cameroun/.

[3] M. Klaus, «letemps.ch,» Melani, 20 Février 2015. [En ligne]. Available: https://www.letemps.ch/economie/question-nest-plus-savoir-serez-hacke. [Accès le 20 Juin 2022].

[4] A. ONANA, «afrimag.net,» AFRIMAG, 15 Février 2018. [En ligne]. Available: https://afrimag.net/cyber-securite-le-cameroun-enregistre-12-800-cyber-attaques/. [Accès le 22 Juin 2022].

[5] Segoor, «segoor.net,» 21 Février 2017. [En ligne]. Available: https://segoor.net/Objectifs_de_la_securite_informatique. [Accès le 28 Juin 2022].

[6] MATROX, «Matrox.com,» 28 Aout 2020. [En ligne]. Available: https://www.matrox.com/fr/video/media/guides-articles/top-ip-kvm-security-elements. [Accès le 29 Juin 2022].

[7] C. Gagné, «blog.present,» 09 Juin 2021. [En ligne]. Available: https://blog.present.ca/fr/5-mythes-mortels-pour-la-s%C3%A9curit%C3%A9-des-pme. [Accès le 24 Juillet 2022].

[8] ISO/IEC JTC 1/SC 27, «iso.org,» 26 02 2018. [En ligne]. Available: https://www.iso.org/fr/standard/73906.html. [Accès le 17 Juillet 2022].

[9] Centre canadien d'hygiène et de sécurité au travail, «cchst.ca,» 15 02 2017. [En ligne]. Available: https://www.cchst.ca/oshanswers/hsprograms/risk_assessment.html. [Accès le 22 Juillet 2022].

[10] M. Buckbee, «varonis.com,» 25 Janvier 2019. [En ligne]. Available: https://www.varonis.com/fr/blog/ids-et-ips-en-quoi-sont-ils-differents. [Accès le 02 Aout 2022].

[11] G. Hiet, «Thèse,» *Détection d'intrusions paramétrée,* pp. 6-15, 19 Decembre 2008.

[12] D. SON, «securityonline.info,» 27 Janvier 2017. [En ligne]. Available: https://securityonline.info/honeypot-honeynet-virtual-attack-defense-system/. [Accès le 28 Juin 2022].

[13] L. GRANGER, «manager-go.com,» 02 Aout 2022. [En ligne]. Available: https://www.manager-go.com/finance/calcul-des-couts.htm. [Accès le 12 Aout 2022].

[14] Perspectives IT, «https://www.silicon.fr/,» 17 Fevrier 2015. [En ligne]. Available: https://www.silicon.fr/blog/pot-de-miel-un-piege-special-hacker. [Accès le 12 Juin 2022].

TABLE DE MATIERES